Titre: Title:	Vers une méthodologie normalisée d'évaluation des solutions RFID en application de sécurité
Auteur: Author:	Pierre Brun-Murol
Date:	2013
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Brun-Murol, P. (2013). Vers une méthodologie normalisée d'évaluation des solutions RFID en application de sécurité [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/1089/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/1089/
Directeurs de recherche: Advisors:	Jose Manuel Fernandez, & Pierre Langlois
Programme: Program:	Génie informatique

UNIVERSITÉ DE MONTRÉAL

VERS UNE MÉTHODOLOGIE NORMALISÉE D'ÉVALUATION DES SOLUTIONS RFID EN APPLICATION DE SÉCURITÉ

PIERRE BRUN-MUROL
DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
AVRIL 2013

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

VERS UNE MÉTHODOLOGIE NORMALISÉE D'ÉVALUATION DES SOLUTIONS RFID EN APPLICATION DE SÉCURITÉ

présenté par : BRUN-MUROL Pierre
en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées
a été dûment accepté par le jury d'examen constitué de :

Mme NICOLESCU Gabriela, Doct., présidente
M. FERNANDEZ José M., Ph.D., membre et directeur de recherche
M. LANGLOIS J. M. Pierre, Ph.D., membre et codirecteur de recherche
M. ROBERT Jean-Marc, Ph.D., membre

À Anne-Lise, mon amour et
soutien de tous les jours...

À mes parents, qui m'ont permis
d'en arriver là...

REMERCIEMENTS

Je tiens tout d'abord à remercier mes deux directeurs de recherche José M. Fernandez et Pierre Langlois pour m'avoir permis de faire cette maîtrise dans le domaine de la sécurité, pour leurs conseils et leur suivi notamment dans la rédaction de ce mémoire et bien sûr pour leur financement.

Je voudrais aussi remercier Jean-Jacques Laurin pour ses conseils avisés dans le domaine des communications radiofréquences et Jérôme Collin pour ses conseils et son aide matérielle continuelle tout au long de ma maîtrise.

Je souhaite encore remercier Joan Calvet pour son aide quotidienne dans mon cheminement, Pier-Luc St-Onge pour son dévouement et Simon Guigui pour son aide précieuse dans les derniers mois de cette maîtrise.

RÉSUMÉ

La technologie d'identification radio-fréquence (RFID) est de plus en plus utilisée dans des applications de sécurité comme le contrôle d'accès et les moyens de paiement. Cependant, elle présente des risques en terme de protection de la vie privée et d'usurpation d'identité. Le but de cette recherche est de mettre en avant ces risques et d'élaborer une ébauche de méthodologie normalisée pour les évaluer.

Dans un premier temps, nous avons reproduit les récents résultats d'autres équipes de recherche sur la solution de contrôle d'accès iClass de la société HID. Pour cela, nous avons notamment implémenté la norme RFID ISO/IEC 15693 sur la carte Proxmark3. Nous avons pu confirmé que la mémoire de certains lecteurs iClass peut être récupérée et qu'elle contient des clés permettant de cloner toutes les cartes du niveau *Standard Security*. Nous avons aussi été en mesure d'implémenter les algorithmes cryptographiques de ce niveau de sécurité sur la Proxmark3, révélés dans un précédent article. Nous pouvons donc parfaitement simuler un lecteur ou une étiquette iClass du niveau *Standard Security*, ou encore espionner une communication.

Dans un deuxième temps, nous avons étudié les limitations physiques des communications RFID. Dans ce cadre, nous avons réalisé la partie émission d'un système permettant d'augmenter la distance de communication entre la carte Proxmark3 et une étiquette. Notre expérience démontre que notre système permet d'activer une étiquette RFID à au moins 81 cm et qu'à cette distance, celle-ci est capable de comprendre les messages envoyés par la Proxmark3 et d'y répondre. Nous avons aussi testé quelques protections de type blindage électromagnétique qui visent à bloquer les communications RFID. Notre expérience montre qu'elles sont efficaces lorsque la carte RFID est complètement insérée dans la protection mais qu'une communication peut être effectuée si la carte ne dépasse que de 12 mm.

Enfin, nous avons élaboré une méthodologie en quatre étapes pour évaluer les risques d'une solution RFID complètement inconnue. Cette méthodologie peut aussi servir de cahier des charges partiel pour la fabrication d'une nouvelle solution.

ABSTRACT

Radio-frequency identification (RFID) technology is widely used for security applications like access control or payment. However, this kind of application poses risks concerning privacy and identity theft. The aim of this study is to highlight these risks and to create a standard methodology to evaluate them.

At first, we reproduced the results of other research teams concerning the HID iClass access control system. In this process, we implemented the RFID standard ISO/IEC 15693 on the Proxmark3 card. We managed to confirm that one can retrieve the memory of some iClass readers and that it contains keys which permit to clone all iClass cards in the *Standard Security* level. We also successfully programed on the Proxmark3 all the cryptographic algorithms of this security level, which were revealed in a previous article. Therefore, we can perfectly simulate an iClass reader or an iClass card from the *Standard Security* level. We can as well spy on iClass RFID communications.

Secondly, we focused on the RFID communication physical limitations. We made the emission part of a system aiming to increase the communication range between the Proxmark3 card and a tag. Our experience shows that our system can power a RFID tag at least at 81 cm and that the tag can understand and answer to the Proxmark3 messages at this range. We also tested some protections using electromagnetic shielding. We showed that there are efficient as long as the card is completely inserted in the protection. However, we managed to establish a communication with a card exceeding the protection by 12 mm.

Finally, we wrote a methodology in four steps to evaluate the risks of an unknown RFID system. This methodology can also be seen as a list of requirements for designing a new RFID solution.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

ASK	Modulation par déplacement d'amplitude (Amplitude Shift Keying)
CVV	Cryptogramme visuel (Card Verification Value)
DMA	Accès direct à la mémoire (Direct Memory Access)
EEPROM	Mémoire morte effaçable électriquement et programmable (Electrically-Erasable Programmable Read-Only Memory)
EMV	Europay Mastercard Visa
FET	Transistor à effet de champ (Field Effect Transistor)
FPGA	Réseau prédiffusé programmable par l'utilisateur (Field Programmable Gate Array)
ICSP	Programmation en série en production (In Circuit Serial Programming)
IEC	Commission électrotechnique internationale (International Electrotechnical Commission)
ISO	Organisation internationale de normalisation (International Standard Organization)
LFSR	Registre à décalage à rétroaction linéaire (Linear Feedback Shift Register)
NFC	Communication en champ proche (Near Field Communication)
PCB	Circuit imprimé (Printed Circuit Board)
RFID	Identification radio-fréquence (Radio-Frequency IDentification)
UART	Émetteur-récepteur asynchrone universel (Universal Asynchronous Receiver Transmitter)
UID	Identifiant unique (Unique IDentifier)
USB	Bus universel en série (Universal Serial Bus)
USRP	Périphérique universel de radio logicielle (Universal Software Radio Peripheral)

CHAPITRE 1

INTRODUCTION

L'identification radiofréquence (RFID) est utilisée dans de nombreux domaines aujourd'hui. Elle permet entre autres de remplacer les codes-barres, de suivre les pièces sur une chaîne de montage et de faire de la gestion des stocks en temps réel. Elle est aussi couramment employée dans des applications plus sensibles comme les titres de transport, les cartes d'accès, les cartes de crédit, les permis de conduire et les passeports. Cependant, la nature sans-fil de cette technologie laisse apparaître de nouvelles menaces. La plus flagrante est l'atteinte à la vie privée car la grande majorité de ces solutions permettent de suivre leurs utilisateurs à leur insu. Mais il est aussi possible de copier une carte d'accès ou d'obtenir les informations d'une carte de crédit sans que son propriétaire ne la sorte de sa poche. Dans ce cadre là, il est nécessaire d'étudier ces applications de sécurité utilisant l'identification radiofréquence pour mieux comprendre les risques qu'elles présentent.

Dans ce chapitre nous expliquons d'abord ce qu'est un système RFID. Ensuite nous considérons les problèmes liés à l'utilisation de cette technologie dans des applications de sécurité. Enfin, nous donnons les objectifs de notre recherche.

1.1 L'identification radio-fréquence

1.1.1 Fonctionnement d'un système RFID

Un système RFID se compose d'au moins deux éléments : un lecteur et une étiquette (Figure 1.1). Les étiquettes sont en général très nombreuses. On les retrouve dans des objets que l'on veut identifier, par exemple une carte à puce ou un objet dans un inventaire. Des caractéristiques souhaitables pour une étiquette sont donc une petite taille, un poids négligeable, un faible coût et une très faible consommation d'énergie. Elles sont composées au minimum d'une antenne et d'un circuit électronique simple permettant de gérer une communication avec un lecteur. Une source d'alimentation peut aussi être présente sur l'étiquette afin d'augmenter son autonomie et ses capacités de communication et de calcul.

Le lecteur est un dispositif qui peut interroger des étiquettes et échanger de l'information avec elles. Les lecteurs peuvent être montés de façon fixe, par exemple à un point de contrôle d'accès d'un édifice, ou encore faire partie d'une unité mobile pouvant être tenue dans la main par un opérateur. Ils sont composés d'une antenne, d'un circuit électronique et d'une source d'alimentation. Les lecteurs sont en général reliés à un système informatique centralisé

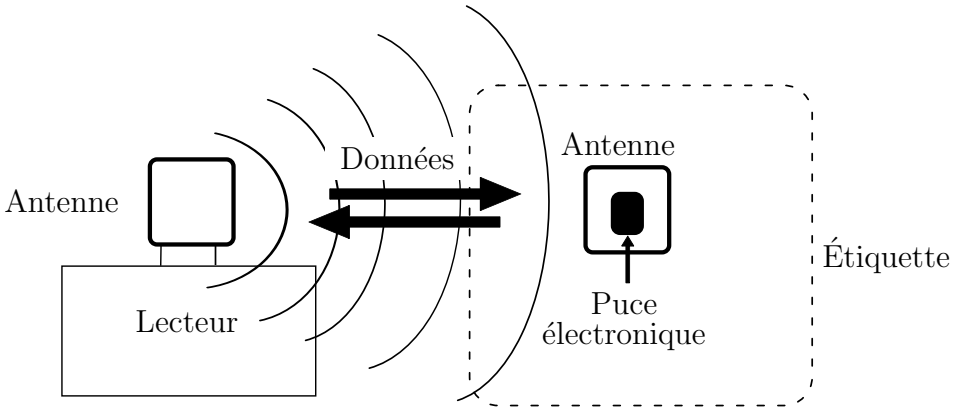

Figure 1.1 Principe de l'identification radio-fréquence

permettant de gérer les informations recueillies des différentes étiquettes.

L'échange d'information entre l'étiquette et le lecteur se fait par ondes électromagnétiques. Lors d'une communication, le lecteur émet une onde porteuse qu'il module pour envoyer des messages à l'étiquette. Pour répondre, l'étiquette utilise la modulation de charge afin de moduler l'onde porteuse émise par le lecteur. Les communications RFID sont régies par des normes qui décrivent de manière exhaustive la communication entre un lecteur et une étiquette, entre autres la fréquence de la porteuse, le format de la modulation, le codage, les protocoles de bas et de haut niveau ainsi que la distance de communication. Par exemple, il existe trois normes pour les communications RFID à une fréquence de porteuse de 13,56 MHz : ISO/IEC 14443a, ISO/IEC 14443b et ISO/IEC 15693. À cette fréquence les distances de communication sont de quelques centimètres.

Les antennes des lecteurs et des étiquettes sont des antennes-boucles pouvant se limiter à quelques spires de fil conducteur. Cette caractéristique permet aux étiquettes n'ayant pas d'alimentation d'utiliser à la place le courant induit dans leur antenne par l'onde émise par le lecteur.

1.1.2 Utilisations de la technologie RFID

La technologie RFID a aujourd'hui de nombreuses applications. Dans la grande majorité de celles-ci, on peut classer leurs objectifs en trois catégories : l'identification, l'authentification et la localisation.

L'**identification** consiste à reconnaitre un objet grâce à l'étiquette RFID qu'il possède. L'identifiant unique de chaque étiquette offre un moyen de distinction entre des objets identiques. Cela se prête très bien à la gestion des stocks [31] ou encore au suivi des pièces sur une chaîne de montage.

L'**authentification** permet de s'assurer de l'identité d'une personne par la possession d'une étiquette RFID. Dans ce cas, il faut que l'étiquette soit difficile voire impossible à reproduire. C'est cet objectif que poursuivent les systèmes de contrôle d'accès utilisant des cartes contenant des étiquettes RFID (cartes RFID). La solution iClass de HID Global est un bon exemple de ce type d'utilisation [11].

La **localisation** consiste à situer une étiquette RFID. Pour cela, il est possible d'utiliser un réseau de lecteurs pouvant communiquer entre eux ou avec un système central pour localiser les étiquettes RFID. En effet, la corrélation des signaux d'une étiquette, reçus par différents lecteurs, permet de la situer précisément. Une autre possibilité est tout simplement de situer plus approximativement l'étiquette comme étant dans le champ d'action d'un lecteur donné. Cette dernière solution est utilisée par exemple dans certains aéroports pour localiser les bagages enregistrés [28].

1.2 Problématique de sécurité en RFID

Du point de vue de la sécurité, la technologie RFID est relativement préoccupante et notamment en ce qui concerne la protection de la vie privée. En effet, une personne pourrait potentiellement être localisée, identifiée et suivie à son insu juste en interrogeant les étiquettes RFID qu'elle possède. Ce risque est d'autant plus important que ces étiquettes s'insinuent de plus en plus dans notre vie quotidienne : passeports, permis de conduire, cartes de paiement, cartes de transport en commun ou encore carte d'accès professionnelle. Pour pallier ce problème, il faut s'assurer que les étiquettes ne dévoilent pas d'informations permettant d'identifier leur porteur, même pendant les communications légitimes.

Cependant, le risque d'atteinte à la vie privée n'est pas le seul problème concernant la technologie RFID. Dans le cadre du contrôle d'accès, il y a des risques d'usurpation d'identité si les étiquettes ne sont pas correctement conçues. Pour éviter cela, il faut qu'il soit difficile de reconstruire de toute pièce une étiquette reconnue comme valide par les lecteurs. Il faut aussi que la copie d'une étiquette soit difficile, même si l'on possède déjà une étiquette authentique. Nous allons voir que ces deux conditions ne sont pas toujours remplies dans les systèmes existants.

1.2.1 Différentes technologies, différents niveaux de problèmes

La technologie RFID regroupe en fait plusieurs technologies dont le principe général reste celui exposé ci-dessus, mais dont les capacités diffèrent. Tout d'abord, il faut distinguer les étiquettes actives, celles qui possèdent une source d'alimentation, des étiquettes passives, celles qui n'en ont pas.

Les **étiquettes passives de 1re génération** ne font aucune authentification avec les lecteurs. Lorsqu'un lecteur les interroge elles envoient directement l'information qu'elles contiennent, sans aucune vérification préalable. Ces étiquettes sont très vulnérables. L'information qu'elles transmettent prend souvent la forme d'un identifiant unique (UID) de quelques dizaines de bits. Il est très facile d'obtenir cet identifiant en reproduisant le ou les messages du lecteur. De plus, on peut aisément simuler une carte en envoyant cet identifiant à partir d'un système générant des ondes radio-fréquence. Ces étiquettes sont donc vulnérables à des atteintes à la vie privée ainsi qu'à des usurpations d'identité. Elles sont néanmoins encore très utilisées aujourd'hui, notamment dans le contrôle d'accès [9]. Ceci s'explique peut être par leur commodité d'utilisation et leur faible coût face à un changement complet de système qui couterait très cher. Du point de vue de la recherche en sécurité, ces étiquettes présentent peu d'intérêt car l'absence d'authentification qui les caractérise les rend forcément vulnérables.

Les **étiquettes passives de 2nde génération** intègrent quant à elles des mécanismes d'authentification mutuelle. Ces mécanismes permettent en théorie d'assurer au lecteur qu'il communique avec une étiquette valide et vice-versa. Cependant, nombre de ces produits ont vu leur sécurité brisée dès qu'une équipe de recherche s'intéresse à elles [5, 7, 14, 21]. La solution de contrôle d'accès iClass de la société HID en est un bon exemple. Les travaux de Meriac [21] ont d'abord démontré la possibilité de cloner certaines cartes d'accès iClass dans le monde entier à partir de l'étude de deux lecteurs iClass. Deux ans après, Garcia *et al.* [7] ont réussi à reconstruire les algorithmes cryptographiques utilisés par cette solution et à briser totalement sa sécurité.

Alors que la cryptographie moderne permet aujourd'hui de sécuriser toute sorte de communication, il est légitime de se demander pourquoi ces solutions RFID n'arrivent pas au même niveau de sécurité. Tout d'abord, les algorithmes de chiffrement utilisés couramment sur les ordinateurs nécessitent une puissance de calcul, et donc une énergie, importante. Cela n'est pas disponible sur une étiquette passive. De plus, le temps de calcul doit être court si on ne veut pas que l'utilisateur soit obligé de tenir sa carte longtemps devant le lecteur.

Ainsi, les fabricants choisissent souvent d'utiliser des algorithmes qu'ils gardent secret. C'est le cas par exemple des solutions iClass de HID Global et Mifare de NXP Semiconductors. Ce concept est appelé « sécurité par l'obscurité » et va à l'encontre des principes de la cryptographie moderne. En effet, d'après les principes de Kerckhoffs, la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clé [15]. Ainsi le cryptosystème, ou algorithme cryptographique, peut être évalué par l'ensemble de la communauté scientifique qui souhaite le mettre à l'épreuve. De cette façon, si l'algorithme n'est pas sûr, il y a plus de chances que cela soit découvert avant qu'une attaque n'ait lieu.

Ces étiquettes passives de 2nde génération ont été présentées par les fabricants comme la réponse aux lacunes de la 1re génération mais l'expérience a montré qu'elles sont autant vulnérables. Les problèmes d'atteinte à la vie privée sont même identiques car toutes les étiquettes de 2nde génération dont nous connaissons l'existence transmettent leur UID avant l'authentification. Même si tous les produits de cette génération ne sont pas encore brisés publiquement, les doutes sont réels concernant la possible sécurité des restants. Néanmoins, comme pour la génération précédente, ces étiquettes sont encore très utilisées et nombre de leurs utilisateurs ne sont pas conscients de leurs faiblesses. La question de savoir s'il est possible de fabriquer des étiquettes sécurisées de ce type n'est donc pas réglée. Cependant, il serait bon que les futurs produits ne répètent pas les erreurs des précédents. C'est pourquoi une méthodologie normalisée d'évaluation des systèmes RFID utilisés en sécurité serait très bénéfique. Elle permettrait de mettre à profit les vulnérabilités découvertes précédemment.

Les **étiquettes actives** ne sont, à notre connaissance, pas utilisées par les applications de sécurité. La présence d'une alimentation entraîne un coût nettement plus élevé qui peut expliquer cette absence. En effet, une étiquette active coûte plus de $25 alors qu'une étiquette passive coûte entre $0.07 et $5 selon la fréquence qu'elle utilise, la quantité de mémoire et les matériaux utilisés. De plus, la durée de vie d'une étiquette active se limite à celle de sa batterie et se situe généralement entre 3 et 8 ans alors que celle d'une étiquette passive est théoriquement illimitée. Les étiquettes actives sont surtout utilisées pour de la localisation à longue distance, notamment d'espèces animales protégées [4].

1.2.2 Outils d'analyse des systèmes RFID

Il existe différents outils pouvant aider à l'analyse des systèmes RFID, opérant à différents niveaux d'abstraction. L'outil le plus bas niveau est très certainement le *Universal Software Radio Peripheral* (USRP), conçu et vendu par la société Ettus Research. C'est un outil très polyvalent permettant de recevoir et d'émettre des signaux jusqu'à une fréquence de 6 GHz. Il est contrôlé par un ordinateur au moyen d'une liaison USB et permet toute sorte d'applications radio-fréquence. Cependant, il faut implémenter soi-même tout le traitement du signal en programmant les FPGA qu'il contient. Une partie du traitement peut aussi être effectuée par l'ordinateur.

À l'opposé, il existe des outils de très haut niveau comme les lecteurs Omnikey de HID Global. Ceux-ci implémentent entièrement plusieurs des normes RFID ainsi que des protocoles de haut niveau propriétaires. Ils permettent de lire certaines étiquettes, de s'authentifier si l'on possède la clé, voire même d'écrire dans la mémoire des étiquettes le permettant. Un kit de développement logiciel peut même être téléchargé sur le site internet de HID. Cependant, ces lecteurs n'offrent pas un contrôle total sur les messages échangés entre le lecteur et les

étiquettes.

Entre ces deux extrêmes se trouvent principalement deux outils : la carte Proxmark3 et la famille de dispositifs OpenPCD. Ils permettent d'espionner une communication RFID ou de simuler une étiquette ou un lecteur. Ils offrent un contrôle total sur les transmissions pour qui le recherche. Néanmoins, il est aussi possible d'utiliser et de modifier les nombreuses fonctionnalités déjà présentes nativement sur ces dispositifs. Le seul bémol est que toutes les normes RFID ne sont pas forcément implémentées nativement. Par exemple, la carte Proxmark3 ne permettait pas de gérer la norme ISO/IEC 15693 lorsque nous avons commencé ce projet de recherche.

Ainsi, la technologie RFID présente des problèmes intéressants dans le domaine de la sécurité. L'existence d'outils adaptés permet d'envisager des travaux de recherche approfondis.

1.3 Objectifs de recherche

Notre recherche s'inscrit dans le cadre de l'évaluation des risques liés à l'utilisation des solutions RFID en sécurité. Nous avons aussi cherché à développer une méthodologie normalisée pour l'évaluation de ces risques.

Plus précisément, les objectifs de recherche abordés dans ce mémoire sont :

1. **Implémenter la norme ISO/IEC 15693 sur la carte Proxmark3**.
   Cette norme est celle utilisée par la solution iClass de HID Global que nous voulions étudier. Il était donc nécessaire d'avoir un outil permettant d'espionner les communications de cette solution ou de simuler un lecteur ou une étiquette.

2. **Reproduire l'attaque de Meriac contre la solution iClass de HID Global** [21].
   Meriac a réalisé une attaque permettant de cloner certaines cartes d'accès iClass. Les conséquences sont importantes et la reproduction de ces résultats permet de les confirmer mais aussi d'obtenir une clé cryptographique utile pour une étude plus poussée de la solution.

3. **Confirmer les résultats de Garcia *et al.* concernant les algorithmes cryptographiques utilisés par la solution iClass de HID** [7].
   Les travaux de Garcia *et al.* ont démontré le très faible niveau de sécurité de la solution iClass dans sa globalité. Encore une fois, l'importance de ces résultats nous a poussé à les reproduire.

4. **Augmenter la distance d'utilisation de la carte Proxmark3**.
   Les attaques existantes sur certaines solutions RFID en application de sécurité représentent un risque pour leurs utilisateurs. Ce risque serait encore plus important si ces attaques pouvaient être exécutées à une distance supérieure à quelques centimètres de la cible. Nous avons donc tenté d'augmenter la distance d'utilisation de la carte Proxmark3 pour démontrer que ce risque plus grand était bien réel.

5. **Tester les contre-mesures de type blindage électromagnétique**.
   Ce type de contre-mesure se trouve facilement sur le marché mais il n'y a pas, à notre connaissance, de données concernant leur efficacité. Il est notamment intéressant de savoir si la carte est protégée lorsqu'elle n'est pas complètement insérée dans sa protection. Nous avons donc sélectionné quelques-uns de ces produits que nous avons testé.

6. **Élaborer une méthodologie normalisée d'évaluation des solutions RFID en application de sécurité**.
   Ce type de méthodologie n'existe pas à notre connaissance. Elle pourrait pourtant être utile aussi bien aux fabricants de solutions RFID qu'aux chercheurs qui étudient leur sécurité. Ainsi, nous avons créé une ébauche de méthodologie à partir de nos travaux et de ceux que nous avons étudiés.

1.4 Plan du mémoire

Ce mémoire est divisé en six chapitres. Afin de répondre à nos questions de recherche, nous étudions dans le chapitre 2 les attaques connues, les contre-mesures existantes ainsi que les méthodologies d'évaluation du risque dans d'autres domaines de la sécurité informatique. Le chapitre 3 traite de notre étude des attaques récemment publiées sur la solution iClass de HID ainsi que les solutions PayPass de Mastercard et PayWave de Visa. Cette étude comprend une analyse de l'effort nécessaire pour mettre en œuvre ces attaques, et donc du risque associé. Dans le chapitre 4, nous présentons notre tentative d'augmentation de la distance de communication entre un lecteur fabriqué par nos soins et une étiquette commerciale. Dans ce même chapitre, nous évaluons l'efficacité des contre-mesures de type cage de Faraday disponibles sur le marché. L'analyse de nos différents travaux ainsi qu'une méthodologie normalisée d'évaluation des risques pour les solutions RFID en sécurité sont présentées dans le chapitre 5. Enfin, nous concluons notre recherche dans le chapitre 6.

CHAPITRE 2

LA TECHNOLOGIE RFID EN SÉCURITÉ

Afin de mieux comprendre l'intérêt de notre travail, il convient d'avoir un aperçu de l'historique de la technologie RFID dans le domaine de la sécurité. Ainsi, nous donnons les concepts de base de l'authentification mutuelle puis nous présentons quelques travaux pertinents concernant des attaques possibles sur certaines cartes RFID. Ensuite, nous abordons des tentatives d'augmentation de la distance maximale de communication. Enfin, nous faisons un rapide survol de différentes solutions de contre-mesures aux attaques existantes.

2.1 Concepts d'authentification mutuelle

Lors d'une communication, l'authentification mutuelle permet d'assurer à chaque interlocuteur que l'autre est bien celui qu'il prétend être. En RFID, cela permet à une étiquette de s'assurer qu'elle communique avec un lecteur légitime mais aussi au lecteur de vérifier que l'étiquette est également légitime. La présence de ce mécanisme de sécurité différencie une étiquette passive de 1re génération d'une étiquette passive de 2nde génération (voir sous-section 1.2.1). Une authentification mutuelle se déroule en cinq étapes illustrées à la figure 2.1 :

1. Alice envoie à Bob un défi.
2. Bob répond à ce défi et envoie un défi à Alice.
3. Alice vérifie la réponse de Bob, si elle est correcte alors Bob est authentifié.
4. Alice répond au défi de Bob.
5. Bob vérifie la réponse d'Alice et si elle est correcte alors Alice est authentifiée.

Les défis sont tels que seuls les personnes connaissant un secret donné peuvent répondre correctement. Ainsi, une authentification mutuelle nécessite un échange préalable de ce secret qui prend généralement la forme d'une séquence de bits appelée « clé ». La réponse au défi est calculée au moyen d'une fonction f telle que :

$$f(cle, defi) = reponse$$

Afin que ce processus d'authentification soit sûr, plusieurs consignes doivent être respectées :

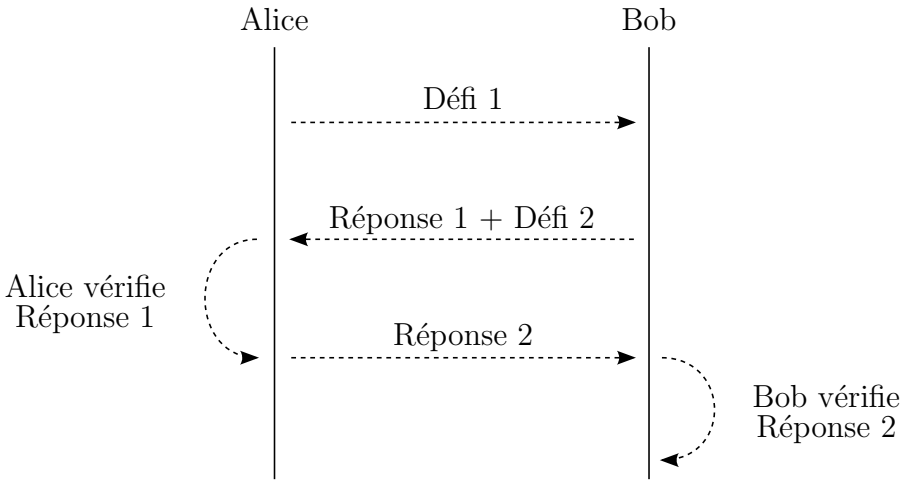

Figure 2.1 Déroulement d'une authentification mutuelle

1. La clé doit demeurer secrète.
2. La fonction f doit être à sens unique, c'est-à-dire qu'on ne peut retrouver facilement la clé en connaissant la réponse et le défi.
3. La clé doit être suffisamment longue pour qu'on ne puisse pas construire de table de correspondance pour un défi donné.
4. La clé doit être suffisamment longue pour qu'une recherche exhaustive dans un temps raisonnable, en connaissant f soit impossible.
5. Le défi doit être aléatoire pour qu'on ne puisse pas le deviner et suffisamment long pour qu'on ne puisse pas construire de table de correspondance pour une clé donnée.

Dans le cadre d'une communication RFID, l'authentification mutuelle pose plusieurs problèmes.

- Dans un système typique, il y a beaucoup d'étiquettes par rapport au nombre de lecteurs. Pourtant, chaque lecteur doit pouvoir authentifier chacune des étiquettes et donc connaître la clé correspondante.
- La génération d'un défi aléatoire est très difficile pour une étiquette passive car cela demande une quantité importante d'énergie et/ou de temps.

Ces difficultés sont gérées différemment selon les fabricants de solution RFID mais pas toujours de façon sécuritaire (voir section 2.2).

2.2 Attaques connues sur des systèmes RFID

2.2.1 Mifare Classic

Mifare Classic est un produit de la société NXP Semiconductors (anciennement Philips Semiconductors). L'étiquette RFID est dans une carte au format carte bancaire. Les applications de ce produit sont très nombreuses, notamment le paiement des transports publics et le contrôle d'accès. Un mécanisme d'authentification et de chiffrement est assuré par l'algorithme de chiffrement symétrique par flux « Crypto-1 » qui utilise une clé de 48 bits. Lors d'une communication, c'est l'étiquette qui envoie le premier défi de l'authentification mutuelle et chacun des deux défis ont une taille de 32 bits. À partir du message du lecteur contenant la réponse au défi de l'étiquette et son propre défi, toute la communication est chiffrée. Pour ce faire, chaque bit des message à envoyer est XOR-é avec un bit généré par l'algorithme Crypto-1. La succession de bits générée par l'algorithme Crypto-1 est appelée « séquence de clé ».

La mémoire de la carte est divisée en plusieurs secteurs et deux clés peuvent être associées à chacun d'eux. Chaque clé donne accès en lecture et/ou en écriture à tout ou une partie du secteur après une authentification réussie. Comme évoqué à la section 2.1, le lecteur doit avoir connaissance de chacune des clés que peuvent utiliser les étiquettes. Lorsque le nombre d'étiquettes dans le système devient important, certaines d'entre elles doivent donc utiliser les mêmes clés.

Les secteurs permettent l'utilisation de la carte pour plusieurs applications différentes. Ainsi, il serait possible d'utiliser la même carte comme moyen de paiement et comme clé d'accès à des installations différentes.

Parmi les solutions RFID utilisant des primitives cryptographiques, Mifare Classic est la plus largement répandue dans le monde lorsque les premières attaques à son encontre sont publiées [25, 24]. La première et principale contribution de ces travaux est la rétro-ingénierie de l'algorithme « Crypto-1 ». En effet, celui-ci était gardé secret par ses concepteurs et n'avait pas d'implémentation logicielle connue. Ces chercheurs ont donc reconstitué l'algorithme à partir de l'étude d'une puce d'une carte Mifare Classic. Ils ont d'abord dissout la carte plastique dans l'acétone pour mettre la puce à nu. Puis, ils ont pris des photos des différents couches de la puce grâce à un microscope optique 500x et en la polissant pour passer d'une couche à l'autre. Un traitement en partie automatisé leur a permis de reconnaitre les portes logiques de la puce, puis d'isoler la partie cryptographique. Enfin, ils ont reconstruit l'algorithme à partir des portes logiques le composant. Après cela, en étudiant le protocole de communication entre une carte et un lecteur à l'aide de l'outil OpenPCD, ils ont découvert comment le système était initialisé. Leur étude a permis de découvrir différentes vulnérabilités

rendant possible des attaques :

Vulnérabilité Mifare 1. La connaissance de l'algorithme et la faible taille de la clé (48 bits) permettent une attaque de force brute.

Vulnérabilité Mifare 2. Le générateur de nombres pseudo-aléatoires de l'étiquette ne dépend que du temps depuis lequel la puce est alimentée et boucle en 0,6 s car son entropie n'est que de 16 bits. Il est de plus réinitialisé au démarrage de la puce. Le même problème de dépendance au temps est présent pour le générateur de nombres pseudo-aléatoires du lecteur.

Vulnérabilité Mifare 3. L'initialisation de l'algorithme combine l'identifiant de la carte (UID) et la clé d'une façon permettant de trouver pour chaque UID une clé générant la même séquence de clé.

Toutes ces vulnérabilités permettent de pré-calculer une table arc-en-ciel (*rainbow table*) pour un identifiant donné. Une fois la clé trouvée pour cet identifiant, il est possible d'en déduire la clé pour d'autres identifiants. La maîtrise des générateurs de nombres pseudo-aléatoires réduit grandement la taille de cette table.

À la même période, de Koning Gans *et al.* [3] avaient eux aussi étudié la solution Mifare Classic et découvert la vulnérabilité du générateur de nombres pseudo-aléatoires (Vulnérabilité Mifare 2). Cependant, ils l'ont découverte en utilisant la carte Proxmark3 sur laquelle ils ont implémenté le protocole ISO/IEC 14443a. Cela leur a permis d'analyser le protocole d'authentification de Mifare Classic. Dans leur travaux, ils exploitent la vulnérabilité du générateur de nombres pseudo-aléatoires ainsi que le fait qu'une partie des données de la mémoire de la carte est connue pour récupérer une partie de la séquence de clé générée par l'algorithme Crypto-1 lors d'une communication entre un lecteur et une carte donnée. La connaissance de cette séquence de clé leur permet de déchiffrer la communication entre ce lecteur et cette carte mais aussi de chiffrer des commandes afin de les envoyer à la carte. La mémoire d'une carte Mifare Classic est divisée en secteurs et leur attaque permet de lire la totalité de tout secteur dont la valeur d'un bloc est connue et en particulier le secteur 0 dont la valeur du bloc 0 peut facilement être retrouvée. Si la valeur d'un bloc n'est pas connue, ils arrivent tout de même à lire une partie de la mémoire de ce secteur. De plus, après avoir récupéré un extrait suffisamment long de la séquence de clé, ils peuvent agir comme un lecteur et envoyer n'importe quelle commande à la carte. Le point important est que tout cela est possible sans aucune connaissance des clés des différents secteurs.

Peu après, Garcia *et al.* [5] ont présenté un article dans lequel ils détaillent très précisément le protocole d'authentification et l'algorithme Crypto-1. Certaines informations révélées étaient absentes de leur précédent article [3] et non divulguées dans l'article de Nohl *et al.* [24]. Ils les ont obtenues en effectuant de nombreuses authentifications avec un simulateur

d'étiquette et un lecteur Mifare. Pour le simulateur, ils utilisent de manière équivalente soit une Proxmark3, soit un appareil construit par eux. Cette connaissance accrue leur a permis de se rendre compte qu'une partie de la séquence de clé générée par l'algorithme Crypto-1 est facilement récupérable puisque le texte clair correspondant est connu ou calculable. Grâce à cela, ils ont mis au point deux attaques permettant d'obtenir la clé secrète utilisée par un lecteur Mifare en utilisant un simulateur d'étiquette. Cela est d'autant plus grave pour un système avec de nombreuses étiquettes puisque dans ce cas certaines d'entre elles partagent les mêmes clés. La 1re attaque exploite deux vulnérabilités :

Vulnérabilité Mifare 4. Les données envoyées par l'étiquette pendant la phase d'authentification influencent directement l'état interne du cryptosystème, le contenu d'un registre à décalage à rétroaction linéaire (LFSR). Cela rend possible la récupération de cet état interne si l'on connaît une partie de la séquence de clé, en utilisant une table de correspondance pré-calculée. La taille de la table est inversement proportionnelle au nombre d'authentifications nécessaires et peut donc être ajustée pour mieux correspondre à un scénario d'attaque précis.

Vulnérabilité Mifare 5. Une fois l'état interne obtenu, une erreur dans la conception de l'algorithme Crypto-1 (dans la fonction de filtrage du LFSR) permet de revenir au contenu initial du LFSR qui n'est autre que la clé secrète.

La 2nde attaque exploite une autre vulnérabilité :

Vulnérabilité Mifare 6. Une erreur de conception de Crypto-1 (encore dans la fonction de filtrage) permet de calculer directement le contenu du LFSR à la fin de l'authentification à condition de connaître une partie de la séquence de clé. Le retour à l'état initial du LFSR se fait de la même façon que pour la première attaque.

Cette attaque est possible en moins d'une seconde.

Toutes les attaques précédentes nécessitent d'avoir accès à un lecteur légitime à un moment ou à un autre autre. Ce n'est pas le cas de celles présentées maintenant et qui sont issues des travaux de Garcia *et al.* [8]. Ces attaques sont basées sur deux vulnérabilités :

Vulnérabilité Mifare 7 Les bits de parité utilisés dans le protocole de Mifare Classic sont calculés sur le texte clair et non sur le texte chiffré. De plus, chaque bit de la séquence de clé qui sert à chiffrer un bit de parité sert aussi à chiffrer un bit de donnée. Enfin, pendant l'authentification, si les bits de parité envoyés par le lecteur sont corrects et que les données d'authentification ne le sont pas, la carte répond par un code d'erreur chiffré. Cela permet d'identifier que les bits de parités sont exacts.

Vulnérabilité Mifare 8 S'il y a des authentifications successives lors d'une communication entre un lecteur et une étiquette Mifare Classic, celles-ci diffèrent légèrement à partir

de la deuxième. Cette différence, associée à la vulnérabilité déjà connue du générateur de nombres pseudo-aléatoires, permet d'obtenir directement une partie de la séquence de clé associée au bloc pour lequel l'authentification est en cours.

Trois des attaques présentées par Garcia *et al.* utilisent la première vulnérabilité (Vulnérabilité Mifare 7) mais de différentes façons. La première est une attaque de force brute qui utilise la vulnérabilité pour obtenir le critère permettant de vérifier si une clé testée est la bonne. La seconde attaque est une attaque à texte chiffré choisi qui permet de réduire de beaucoup le temps de calcul nécessaire après l'attaque aux dépens d'un plus grand nombre d'échanges avec la carte Mifare Classic. La troisième s'appuie sur une table pré-calculée et ne nécessite qu'environ deux minutes de communications avec la carte. Ces attaques exploitent la même vulnérabilité mais permettent de s'adapter à différents scénarios en fonction du temps et des ressources disponibles dans les différentes phases de l'attaque. Si un attaquant a déjà obtenu la clé d'un secteur de la carte, en utilisant l'une des trois attaques précédentes par exemple, la dernière attaque profite des deux vulnérabilités (Vulnérabilités Mifare 7 et 8) pour obtenir la clé de n'importe quel autre secteur en moins d'une seconde. Une fois la clé d'un secteur connu, il est possible de lire toutes les données de ce secteur. Ainsi il est possible de cloner entièrement une carte Mifare Classic, sans avoir accès à un lecteur légitime.

Tous les travaux précédents démontrent clairement que le niveau de sécurité de l'algorithme Crypto-1 est très faible. La taille de sa clé, 48 bits, est trop petite par rapport aux puissances de calcul actuelles. Les découvertes des différentes équipes de recherche ont même montré que des erreurs de conception de l'algorithme diminuent la taille effective de la clé en dessous des 48 bits. On peut se demander pourquoi les concepteurs ont utilisé une taille de clé si petite. Peut-être ont-ils pensé que ce défaut serait compensé par le secret de l'algorithme mais il n'en est rien puisque le secret a été révélé par une équipe de recherche. Les deux autres principaux défauts de conception sont :

- Les générateurs de nombres pseudo-aléatoires ne dépendent que du temps depuis lequel ils sont alimentés (Vulnérabilité Mifare 2). Cela diminue très fortement l'entropie des messages durant l'authentification et donc le nombre de calculs nécessaires pour une attaque réussie.
- Certains bits de la séquence de clé sont utilisés deux fois dans le chiffrement (Vulnérabilité Mifare 7). Cela divulgue une partie de l'information chiffrée et viole les principes du chiffrement par flux bit à bit.

D'un point de vue méthodologique, on peut remarquer que Nohl et Plötz [25] ont innové dans leur travaux. Ils ont démontré qu'il était possible de révéler un algorithme cryptographique à partir d'une puce en silicone l'implémentant, avec des moyens relativement simples et un microscope optique 500x. Il est donc inutile que les fabricants de solutions RFID

tentent d'utiliser le secret de leurs algorithmes comme moyen de sécurité. On peut aussi remarquer que tous ces travaux n'auraient pas été possible sans outils tels que la Proxmark3 et l'OpenPCD qui ont permis d'analyser les communications RFID et de simuler des étiquettes et des lecteurs.

2.2.2 HID iClass

La solution iClass est un produit de la société HID Global qui prend aussi la forme d'une carte de format bancaire. Elle est principalement utilisée dans le contrôle d'accès mais aussi pour le paiement, dans certains systèmes comme FreedomPay. La sécurité de ce produit est assurée par un algorithme propriétaire gardé secret par HID Global qui utilise une clé de 64 bits et assure l'authentification mutuelle de la carte et du lecteur[11].

Comme pour la solution Mifare Classic, lors d'une communication c'est l'étiquette qui envoie la première son défi de 64 bits. Le défi du lecteur est de 32 bits et contrairement au modèle d'authentification mutuelle présenté à la section 2.1, chacune des réponses aux défis dépend des deux défis et non d'un seul. Ceci est utilisé pour augmenter l'entropie en entrée de l'algorithme propriétaire qui calcule les réponses. De plus, comme l'étiquette ne possède pas de générateur de nombres pseudo-aléatoires c'est le lecteur qui écrit dans la mémoire de l'étiquette, à la fin de chaque authentification, le défi à utiliser la prochaine fois.

La mémoire de la carte est divisée en applications et chacune d'entre elles est protégée par une clé de 64 bits. Plus précisément, pour chaque application, il existe une clé maître de laquelle est dérivée une clé dite « diversifiée », différente pour chaque étiquette iClass et stockée sur celle-ci. Ainsi, la connaissance de la clé maître suffit au lecteur pour authentifier toutes les étiquettes.

La première application de la carte est celle utilisée par HID pour conserver les informations de contrôle d'accès. Une partie de ces données sont chiffrées avec une clé 3DES (128 bits). Cette application est proposée avec trois niveaux de sécurité différents [1] : *Standard Security*, *Elite* et *Field Programmer*.

- Dans le niveau *Standard Security*, toutes les cartes de tous les clients dans le monde entier partagent la même clé maître (et la même clé 3DES).
- Dans le niveau *Elite*, une clé maître (et une clé 3DES) est associée à chaque client mais c'est HID Global qui gère le chemin de clés. De plus, l'algorithme de diversification de clé est différent que celui du niveau *Standard Security*.
- Dans le niveau *Field Programmer*, c'est la même chose que le niveau *Elite* sauf que le client gère son propre chemin de clés.

A notre connaissance, les premiers travaux de recherche sur ce produit sont ceux de Meriac et Plötz [22] présentés lors du 27^{e} Chaos Communication Congress et dont une partie

fait l'objet d'un rapport technique publié le jour de la présentation [21]. L'intérêt majeur de ces travaux est la possibilité d'obtenir la clé maître du niveau *Standard Security* et toutes les conséquences qui en découlent. Pour cela Meriac [21] a acheté des lecteurs iClass RW400 sur eBay dans le but d'obtenir la clé maître qu'ils contenaient forcément. En les ouvrant, il découvre que ces lecteurs sont opérés par un microcontrôleur de Microchip, un PIC18F452. De plus, six connecteurs sont accessibles à l'arrière du boîtier et se révèlent être les connecteurs de programmation en production (ICSP) du PIC. Ceux-ci servent à déboguer ou à reprogrammer le PIC avec un équipement comme le PICkit2 de Microchip. Avec ce dernier, une tentative de lecture de la mémoire du PIC révèle que celle-ci est protégée en lecture. Cependant, après étude des spécifications de programmation des PIC18F, il s'avère qu'il est possible d'écraser indépendamment les blocs de mémoire du PIC (**Vulnérabilité iClass 1**). Néanmoins, les commandes nécessaires à cette opération ne sont pas accessibles avec les équipements commerciaux de Microchip comme le PICkit2. Ainsi Meriac a fabriqué un équipement permettant d'envoyer ces commandes au PIC ainsi que d'écrire dans la mémoire de celui-ci. En remplaçant le premier bloc mémoire par un programme qui envoie la totalité de la mémoire par le port série, il a obtenu toute la mémoire sauf le premier bloc. Sur un autre lecteur, en remplaçant tout sauf le premier bloc par le même programme, il a récupéré la partie manquante de la mémoire du PIC. Une fois la clé maître et la clé 3DES facilement identifiées, Meriac a utilisé un lecteur Omnikey de HID ainsi qu'une application fournit par HID dans le kit de développement Omnikey pour vérifier qu'il peut effectivement lire et écrire dans la mémoire d'une carte iClass. L'auteur a effectivement réussi à lire le contenu de la première application d'une carte iClass et à modifier la valeur des blocs. En plus de cette importante vulnérabilité, Meriac et Plötz [22] ont identifié des problèmes de sécurité dans le protocole de communication de la solution iClass ainsi que dans la façon de stocker les données sur les cartes :

Vulnérabilité iClass 2 Lorsque la carte répond à une commande du lecteur, rien n'authentifie cette réponse. Ainsi une attaque *man-in-the-middle* est possible une fois l'authentification passée.

Vulnérabilité iClass 3 Il est possible de copier les blocs de données chiffrés d'une carte à une autre car le chiffrement 3DES est utilisé en mode ECB.

L'ensemble de ces résultats permet donc de cloner les données d'authentification d'une carte iClass. Cela serait même possible sans la connaissance de l'algorithme de chiffrement utilisé. Il faut noter que les modèles récents de lecteur iClass n'utilisent pas le même PIC et ne présentent pas cette vulnérabilité (Vulnérabilité iClass 1). Cependant, la même clé maître est utilisé pour le niveau *Standard Security*.

Ultérieurement, Garcia *et al.* [6] ont démontré qu'il était possible d'obtenir la clé maître

d'une toute autre façon. Pour cela ils se sont intéressés à l'algorithme de diversification. Afin de pouvoir observer les différences dans les communications d'une carte et d'un lecteur en fonction de la clé maître, ils avaient besoin de pouvoir changer celle-ci. Cela est notamment possible à l'aide d'un lecteur Omnikey en utilisant le mode *Secure Mode*. Pour pouvoir l'utiliser, il faut avoir une clé 3DES K_{CUW} permettant d'établir une communication sécurisée entre l'ordinateur et le lecteur Omnikey. Cependant cette clé n'est disponible qu'en signant un accord de non-divulgation avec HID Global. La solution naviGO de HID utilise une application sur les carte iClass, autre que la première, pour fournir un moyen d'ouvrir une session Windows. Garcia *et al.* en ont donc déduit que cette solution pouvait changer les clés maîtres des applications et ont ainsi trouvé K_{CUW} dans un fichier binaire non-protégé d'une version d'essai de ce produit (**Vulnérabilité iClass 4**). Grâce à cela, ils ont créé une librairie *iClassified*, disponible sur le site `www.proxmark.org`, permettant d'envoyer des commandes à un lecteur Omnikey dans le mode *Secure Mode*.

En changeant la clé maître et en observant les communications entre l'ordinateur et le lecteur Omnikey, ils ont découvert que lors de la mise à jour de la clé diversifiée de la carte, c'est le ou-exclusif de la nouvelle et de l'ancienne clé diversifiée qui est envoyée à la carte. Les informations sur le produit PicoPass de Inside Secure [12], sur lequel est basée la solution iClass, suggèrent que l'algorithme de diversification de clé consiste à chiffrer l'identifiant de la carte avec DES et la clé maître puis à appliquer une fonction de fortification de clé *hash0*. Cela est confirmé facilement par Garcia *et al.*.

De plus, dans le même fichier binaire qui contenait K_{CUW}, ils ont découvert la clé maître par défaut de la deuxième application des cartes iClass. Avec tout ce matériel, les auteurs ont monté une expérience leur permettant de voir l'influence d'un changement de bit en entrée de *hash0* sur sa sortie. En collectant ces informations pour un grand nombre d'entrées puis en les analysant, ils ont réussi à retrouver l'expression de la fonction de fortification. Son analyse montre qu'elle diminue l'entropie de son entrée de 2,2 bits et qu'en moyenne une sortie de cette fonction n'a que 4,2 pré-images (**Vulnérabilité iClass 5**). Garcia *et al.* ont donc exprimé la fonction inverse $hash0^{-1}$ et monté une attaque permettant d'obtenir la clé maître en inversant toute la fonction de diversification. La complexité de cette inversion se ramène à celle de briser DES. La validité des clés maîtres acquises ainsi pour les deux premières applications des cartes iClass a pu être vérifiée en les comparant à la clé obtenue dans le binaire et à celle récupérée dans la mémoire d'un lecteur en suivant la démarche de Meriac [21].

Les deux travaux précédents permettent d'obtenir la clé maître. Ceci rend possible le clonage des informations d'authentification utilisées par les cartes iClass du niveau *Standard Security*. Pour ce faire, il faut utiliser un lecteur Omnikey ou tout autre dispositif implémen-

tant le protocole iClass et permettant de personnaliser la clé maître utilisée. Ces résultats compromettent sévèrement, voire annihilent, la sécurité procurée par les cartes iClass du niveau *Standard Security*.

Il faut noter que toutes ces vulnérabilités ont été découvertes sans la connaissance de l'algorithme d'authentification propriétaire de HID. De plus, une fois celui-ci révélé par les travaux de Garcia *et al.* [7], de plus graves attaques ont été découvertes. En effet, ces chercheurs ont effectué la rétro-ingénierie du micrologiciel d'un lecteur iClass RW400, obtenu par la méthode de Meriac [21], et ont ainsi révélé tout le protocole de la solution iClass. En plus de donner des formules mathématiques des algorithmes d'authentification et de diversification (des deux niveaux de sécurité), leurs travaux révèlent des faiblesses permettant deux nouvelles attaques. Celles-ci sont effectuées à l'aide d'une Proxmark3 et d'un ordinateur uniquement. La première d'entre-elles est une autre façon d'obtenir la clé maître du niveau *Standard Security* et exploite quatre vulnérabilités :

Vulnérabilité iClass 6 L'étiquette ne possède pas de générateur pseudo-aléatoire. C'est le lecteur qui met à jour, à chaque communication, la valeur servant de défi pendant l'authentification. L'étiquette ne vérifie pas que la valeur a changé.

Vulnérabilité iClass 7 Si la clé diversifiée utilisée avec l'algorithme d'authentification est de la forme $k = \alpha_0\beta \dots \alpha_7\beta$ avec $\alpha_i \in \{0,1\}^5$ et $\beta \in \{0,1\}^3$, alors la sortie de l'algorithme ne dépend que de β.

Vulnérabilité iClass 8 Lorsqu'un lecteur authentifié envoie une commande d'écriture valide ciblant le bloc mémoire contenant la clé diversifiée, la nouvelle valeur de ce bloc est le ou-exclusif de l'ancienne et de celle envoyée par le lecteur. Ce fonctionnement empêche certes de déduire la nouvelle clé en observant la communication mais permet à un lecteur de modifier partiellement la clé diversifiée.

Vulnérabilité iClass 9 Une fois authentifié avec l'application 1 d'une carte iClass, si un lecteur tente de lire un bloc mémoire de l'application 2, la carte ne lui renvoie qu'une séquence de bits à '1'. Cependant, le lecteur ne perd pas ses droits d'accès à l'application 1 et l'algorithme d'authentification de la carte utilise par la suite la clé diversifiée de l'application 2.

Vulnérabilité iClass 5 L'algorithme de diversification de clé du niveau *Standard Security* peut être inversé d'après les travaux de Garcia *et al.* [6].

L'attaque nécessite la connaissance de la clé maître de l'application 2, disponible en ligne [6], et consiste dans un premier temps à obtenir la clé diversifiée de l'application 1 d'une carte. Pour cela, l'attaquant met à profit les quatre premières vulnérabilités (Vulnérabilités 6, 7, 8 et 9) et a besoin d'espionner une communication légitime entre un lecteur et une carte. Il lui

faut aussi pouvoir communiquer avec la même carte pendant environ six heures. En incluant les calculs post-communication, cette première partie de l'attaque peut être effectuée en une journée. Ensuite, il suffit d'inverser l'algorithme de diversification.

La seconde attaque permet d'obtenir la clé maître d'un lecteur iClass du niveau de sécurité *Elite*. L'algorithme de diversification de ce niveau consiste à effectuer un premier calcul sur la clé maître qui donne une nouvelle clé. Celle-ci est ensuite diversifiée de la même façon que pour le niveau de sécurité normal. Le problème est que ce premier calcul réduit drastiquement la sécurité de la diversification. En effet, il contient deux vulnérabilités (**Vulnérabilités iClass 10 et 11**) permettant d'obtenir la clé maître en moins de cinq secondes. Les détails de ces deux vulnérabilités ne sont pas discutés ici car trop techniques mais le problème de fond est que le premier calcul sur la clé maître devrait être à sens unique et ce n'est pas le cas.

Tous les travaux sur la solution iClass de HID Global présentés précédemment montrent, une fois de plus, que la sécurité par l'obscurité n'apporte rien. Il est aussi possible de s'interroger sur la pertinence d'utiliser l'algorithme DES alors qu'il est vulnérable à des attaques de type *bruteforce* depuis la fin des années 1990 [2]. Ceci, ainsi que les erreurs de conception de la diversification de clé dans le niveau *Elite*, auraient tout de suite été pointés du doigt si les algorithmes avaient été rendus publics. L'évaluation par les pairs est un critère de choix à privilégier. De plus, comme Garcia *et al.* le soulignent dans leur conclusion, l'ajout d'algorithmes n'apporte pas forcément plus de sécurité. En effet, dans la diversification de clé du niveau *Elite*, c'est le traitement ajouté pour ce niveau qui le rend encore plus vulnérable que le niveau *Standard Security*.

En ce qui concerne les méthodes d'étude de ce produit, on peut remarquer comme pour Mifare Classic deux approches différentes et complémentaires. La première est axée sur le matériel, et l'autre sur l'étude du protocole de communication.

2.2.3 Mastercard PayPass / Visa PayWave

La facilité d'utilisation de la technologie RFID a conduit les compagnies de carte de crédit Mastercard et Visa à intégrer des étiquettes RFID dans certaines de leurs cartes. Cette technologie s'appelle PayPass chez Mastercard et PayWave chez Visa. Ces deux technologies sont compatibles avec la norme Europay Mastercard Visa (EMV), qui cherche à assurer la sécurité et l'interopérabilité des principaux systèmes de carte de crédit au monde. Elles sont aussi basées sur la norme RFID ISO/IEC 14443. PayPass et PayWave permettent aux possesseurs de ces cartes de crédit de payer en faisant juste passer leur carte devant un lecteur compatible.

Cependant, certains travaux démontrent que les échanges RFID entre la carte et le lecteur

ne sont pas toujours sécurisés. En effet, dans l'émission télévisée « La facture » diffusée le 10 janvier 2012 sur la chaîne canadienne Radio Canada, Daniel Boteanu, expert en sécurité chez Okiok, démontre la vulnérabilité de cette technologie. L'expérience qu'il présente est assez simple. Il a acheté sur eBay, pour moins de $100, un lecteur compatible PayPass/PayWave qui se branche habituellement sur une caisse enregistreuse. Ensuite, lorsqu'il alimente ce lecteur, celui-ci est capable d'interroger des cartes de crédit de manière autonome et il envoie les informations recueillies par son câble série. Cependant, ce n'est pas une caisse enregistreuse qui est branchée à l'autre bout du câble mais du matériel permettant de récupérer ces informations et de les afficher sur la tablette tactile de Daniel Boteanu. Les informations qui transitent dans ce câble ne sont absolument pas chiffrées. De plus, Daniel Boteanu insiste bien sur le fait que ce type de lecteur est accessible à n'importe qui sur Internet. Aucune vérification n'est faite pour savoir si l'on tient un commerce légitime par exemple.

Dans une présentation faite à Paris au Hackito Ergo Sum 2012, Lifchitz [20] explique qu'en fait même la communication RFID est faite sans chiffrement. N'importe qui peut donc espionner les échanges entre une carte de crédit et un lecteur légitime, avec une Proxmark3 par exemple, et obtenir toutes les informations recueillies par le lecteur. Le présentateur démontre aussi qu'il est possible d'interroger directement la carte puisqu'il n'y a pas non plus d'authentification. Il fait d'ailleurs une démonstration avec une application Android qu'il a créée. Ainsi, une personne mal intentionnée pourrait voler les informations bancaires des personnes qu'il approche avec son téléphone.

Les informations obtenues dans les travaux présentés sont :

- le nom, le prénom et le sexe du porteur de carte ;
- le numéro de la carte de crédit ;
- la date d'expiration ;
- les données de la bande magnétique ;
- l'historique des transactions.

Ces informations suffisent à passer des achats sur certains sites internet qui ne demandent pas le CVV, comme le démontrent les journaliste dans l'émission de « La facture ». Il est aussi possible d'écrire les informations de la bande magnétique sur une autre carte et d'utiliser celle-ci pour effectuer des achats dans des commerces qui n'ont pas de terminaux de paiement qui lisent la puce électronique de la carte. C'est notamment le cas de tous les commerces des États-Unis et d'une partie de ceux du Canada. Enfin, comme toutes les étiquettes RFID qui envoient un identifiant avant authentification, il est possible de traquer une personne grâce à sa carte de crédit RFID.

Il est aussi important de remarquer que même si la communication RFID était correctement chiffrée l'attaque de Daniel Boteanu serait toujours possible. Pour contrer cette attaque,

il faudrait chiffrer la communication entre le lecteur PayPass/PayWave et la caisse enregistreuse. Cependant, cela nécessiterait sûrement de changer la caisse enregistreuse et n'est donc pas envisageable pour tous les commerces. Ainsi, même une très grande sécurité au niveau de la communication RFID serait futile si les lecteurs sont toujours disponibles aussi facilement sur Internet.

2.3 Distance de communication maximale

La distance de communication maximale est un facteur critique dans la technologie RFID. En effet, même si les normes prévoient la possibilité que plusieurs étiquettes soient dans le champ d'action d'un lecteur, en pratique, on doit tenir compte de facteurs reliés à l'utilisation du système. Une solution de contrôle d'accès, par exemple, doit permettre de valider l'identité de la personne qui est juste devant le lecteur et non pas d'une autre personne passant dans le couloir. Il en est de même pour les cartes de crédit. L'identité du payeur doit être déterminée sans équivoque afin que les frais soient portés au bon compte. C'est pour ces raisons pratiques que les lecteurs RFID des solutions opérant à 13,56 MHz, principalement utilisées pour le contrôle d'accès et le paiement, ont des distances maximales de communication de quelques centimètres [11, 26].

Au vu des attaques existantes sur certaines solutions RFID (voir section 2.2), il est légitime de se demander si cette distance de communication peut être augmentée. En effet, le risque lié à une attaque serait d'autant plus grand que la distance à laquelle elle est faisable serait importante. Une équipe de recherche a même proposé un système qui contournerait n'importe quelle authentification ou chiffrement d'une communication RFID [16]. En effet, leur idée est de faire une attaque par relais en utilisant deux appareils (voir figure 2.2). Le premier, appelé fantôme (de l'anglais *ghost*), communique avec un lecteur RFID légitime. Le second, appelé sangsue (de l'anglais *leech*), communique quant à lui avec une étiquette légitime. Ces deux appareils ne sont en fait que des relais communiquant entre eux par un canal rapide, comme l'Internet. Les messages du lecteur légitime sont reçus par le fantôme qui les transmet à la sangsue. Celui-ci les envoie à l'étiquette en simulant un lecteur. Les messages de l'étiquette sont transmis de la même façon au lecteur légitime.

Ainsi, ce système permettrait d'utiliser par exemple la carte de crédit RFID de quelqu'un d'autre pour payer une note, même si cette personne est à des kilomètres du terminal de paiement. Selon les auteurs, la distance entre la sangsue et le fantôme est illimitée. Cependant, ils considèrent que les distances de communication RFID conventionnelles de quelques centimètres sont une limitation puisqu'elles diminuent la discrétion de l'attaque. Ils proposent donc dans leur article plusieurs solutions pour améliorer ces distances. Leurs travaux

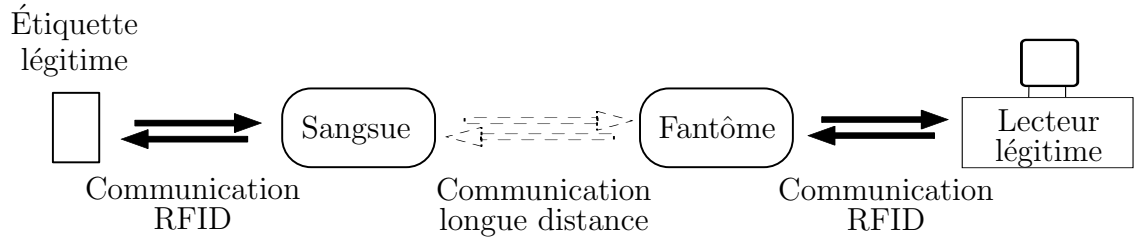

Figure 2.2 Schéma de l'attaque par relais proposée par Kfir et Wool [16]

se basent notamment sur des simulations utilisant le modèle NEDAP, implémenté en langage C. Ce modèle permet de représenter les effets inductifs des systèmes RFID. Il est important de noter que tous ces travaux ont été effectués avec la norme ISO/IEC 14443b. Les auteurs affirment par ailleurs que les résultats sont très similaires pour la norme ISO/IEC 14443a.

Pour la communication entre le fantôme et le lecteur légitime, les auteurs ont considéré deux scénarios de bruit différents.

Bruit d'origine humaine : C'est un bruit « standard » suivant le modèle du secteur radio-télécommunication de l'Union Internationale des Télécommunications.

Bruit d'interférence RFID : Ce bruit représente la présence d'autres lecteurs RFID que celui ciblé par l'attaque.

Le fantôme possède une source d'alimentation et ne tire donc pas son énergie de l'onde émise par le lecteur. Cela permet une distance plus importante pour une communication depuis le lecteur vers le fantôme. En effet, les simulations des auteurs donnent une distance possible de 50 m pour le modèle du bruit d'origine humaine, dans ce sens de la communication. Pour le modèle du bruit d'interférence RFID, il faut que le fantôme soit environ trois fois plus proche du lecteur que les sources d'interférences. En ce qui concerne le sens de communication du fantôme vers le lecteur, il faut tout d'abord remarquer que la modulation de charge d'une étiquette est identique à une modulation d'amplitude « classique » du point de vue du lecteur. Or, si le fantôme utilise la modulation d'amplitude « classique », la distance de communication maximale est la même pour les deux sens de communication.

Pour la communication entre l'étiquette et la sangsue, Kfir et Wool n'ont considéré cette fois-ci qu'un seul scénario de bruit. Il s'agit de la présence d'un autre système RFID émettant à la limite maximale de puissance permise par la réglementation et à une distance de 100 m. Afin d'augmenter la distance de communication entre l'étiquette et la sangsue, les auteurs proposent trois améliorations :

1. L'augmentation de la taille de l'antenne cadre de la sangsue et du courant la parcourant.
2. La retransmission des messages et leur traitement logiciel.

3. La retransmission des messages puis leur traitement par entrelacement et filtrage.

L'amélioration 1 permet d'augmenter la taille du champ dans lequel l'étiquette peut être activée. Dans leurs simulations, les auteurs ont fait varier le courant entre 1 et 4 A. Ils ont remarqué que pour cet intervalle de valeurs, la taille optimale de l'antenne était toujours autour de 0,4x0,4 m. Les améliorations 2 et 3 visent à diminuer le nombre d'erreurs de réception dues au bruit.

Les résultats obtenus grâce à ces améliorations sont donnés au tableau 2.1. Il faut noter que le coût ne comprend pas l'équipement permettant à la sangsue et au fantôme de communiquer entre eux. Ainsi, les simulations annoncent une distance maximale de 55 cm entre la sangsue et l'étiquette mais cela demande plus de $5000 en matériel et beaucoup de connaissances en traitement du signal.

Tableau 2.1 Résultats des améliorations de la sangsue d'après les travaux de Kfir et Wool [16]

Améliorations	Distance maximale	Coût	Connaissances nécessaires
1	40 cm	< $100	Moyennes
1 + 2	50 cm	< $100	Hautes
1 + 3	55 cm	> $5000	Très hautes

Ces travaux, même s'ils restent uniquement théoriques, ont le grand mérite d'essayer de poser une limite à la distance de communication maximale dans un système RFID. On peut cependant s'interroger sur l'intérêt pratique du scénario du bruit d'origine humaine pour la distance entre le lecteur légitime et le fantôme. En effet, en application de sécurité, il est courant que plusieurs lecteurs RFID soient proches et c'est donc le scénario du bruit d'interférence RFID qui serait le plus réaliste. Il est donc fortement probable que la limite des 50 m soit très difficile à atteindre en pratique car cela signifierait une absence d'autre lecteur RFID dans un rayon de 150 m. Néanmoins, la plupart des scénarios d'attaque ne nécessitent pas que le fantôme soit loin du lecteur. Aussi bien pour contourner un système de contrôle d'accès que pour effectuer un paiement frauduleux, l'attaquant et donc le fantôme, doivent être proches du lecteur pour ne pas éveiller les soupçons.

Le travail de Kirschenbaum et Wool [19] est en fait la réalisation d'un appareil pouvant servir le rôle de la sangsue. Cet appareil, qu'ils nomment copieur (de l'anglais *skimmer*), peut aussi servir de manière autonome pour interroger des étiquettes dépourvues de sécurité et obtenir leurs informations. Il implémente la norme ISO/IEC 14443a. Le copieur est portable et ne nécessite que des connaissances de base et du matériel d'amateurs d'électronique selon les auteurs. De plus, sa conception n'a besoin que d'un budget d'environ $100, comme annoncé par Kfir et Wool [16]. Cet appareil est principalement composé de cinq éléments :

Le lecteur ISO 14443a Cet élément est en fait un microcontrôleur S4100 de Texas Instrument. Il implémente notamment la norme ISO/IEC 14443a et peut normalement être connecté directement à une antenne. Cependant, il n'est pas capable de généré un courant suffisamment important pour atteindre la distance de communication voulue.

L'amplificateur de puissance Son élément principal est un transistor FET de puissance et il permet de générer un courant important. Il est branché à la place de l'antenne sur le microcontrôleur S4100.

L'antenne Elle est composée d'un tube de cuivre de diamètre 8 mm qui forme un cercle de 39 cm de diamètre. Elle est accompagnée d'un circuit d'adaptation d'impédance.

Le récepteur Cette partie du système permet au microcontrôleur S4100 de lire les réponses des étiquettes sans avoir à soutenir les fortes tensions aux bornes de l'antenne. Il sert d'interface qui abaisse la tension sans influencer le facteur de qualité de l'antenne.

La source de tension Dans sa version portable, le copieur est alimenté par une batterie rechargeable Plomb-Zinc de 7 A h. Pour les travaux en laboratoire, les auteurs ont utilisé une source de tension régulée.

Les auteurs ont rencontré des difficultés pour faire l'adaptation d'impédance entre l'amplificateur de puissance et l'antenne. Ils ont essayé d'utiliser la méthode décrite dans l'annexe B de la norme ISO/IEC 10373-6 mais n'ont pas obtenu de bon résultats. Selon eux, malgré le fait que cette méthode soit spécifique à la technologie RFID, elle n'est pas adaptée à des amateurs d'électronique et leur matériel. C'est pourquoi ils ont utilisé un mélange de deux autres méthodes pour évaluer leur adaptation d'impédance.

- La première consiste à amener dans le champ produit par l'antenne du copieur une deuxième antenne boucle. En reliant celle-ci à un wattmètre de fabrication personnelle, les auteurs avaient accès à une mesure indirecte de la puissance transmise par l'amplificateur à l'antenne du copieur.
- La seconde est itérative est consiste tout simplement à tenter une communication entre le copieur et une étiquette de plus en plus éloignée.

En utilisant ces deux méthodes d'adaptation d'impédance les auteurs ont réussi à effectuer une communication entre une étiquette et le copieur distants d'environ 25 cm.

Cette expérience prouve qu'il est possible d'interroger une étiquette RFID à une distance nettement supérieure à quelques centimètres. De plus, la conception du matériel nécessaire à cette expérience n'est pas très coûteuse, environ $100. Ainsi, les attaques déjà possibles sur les étiquettes de certaines solutions RFID sont rendues plus faciles et leur risque associé est donc plus grand. Il faut tout de même noter que les travaux précédents ont tous été effectués

avec des étiquettes des normes ISO/IEC 14443a et 14443b. Même s'il est possible que des résultats identiques soient atteignables avec la norme ISO/IEC 15693, rien ne le prouve.

2.4 Contre-mesures existantes

Les sections 2.2 et 2.3 ont mis en avant les risques importants que présentent certaines solutions RFID en application de sécurité. Cependant, il existe des contre-mesures qui permettent de réduire ces risques. Certaines d'entre elles représentent une surcouche de sécurité alors que d'autres nécessitent une modification importante de la solution RFID.

Le premier exemple de surcouche de sécurité est la présence d'un interrupteur connecté à l'étiquette RFID [13]. Si le propriétaire ne presse pas cet interrupteur, celui-ci interdit toute communication de la part de l'étiquette et bloque donc les attaques possibles. De plus, personne ne peut lire les données contenues dans la mémoire de l'étiquette sans intervention de son propriétaire, même en connaissance de tous les algorithmes cryptographiques et de leurs clés respectives. Malgré l'efficacité de type de protection, il n'est pas utilisé par les solutions RFID en application de sécurité que nous connaissons, peut-être à cause d'un coût important de production. Il est donc nécessaire de trouver des protections efficaces et accessibles aux utilisateurs finaux.

Le second exemple de surcouche de sécurité est l'utilisation d'un blindage électromagnétique, comme dans les produits des sociétés Identity Stronghold, DIFRwear ou Flipside Wallet. Ce type de blindage permet de protéger des objets de champs électromagnétiques. Il consiste à interposer entre la source du champ et l'objet une barrière composée de matériaux conducteurs électriques. Dans le cas qui nous intéresse, il est utilisé pour empêcher les ondes radiofréquences d'atteindre l'étiquette RFID. Ce blindage peut être intégré à toute sorte de produits comme des portefeuilles, des étuis de carte ou des portes-badges dont le prix varie entre \$3 et \$50. Dans ce cas, cela permet aux utilisateurs finaux de se protéger même si les produits RFID qu'ils utilisent sont vulnérables.

S'il est efficace, le blindage a donc le même effet que l'interrupteur, il bloque toutes les communications. Pour évaluer l'efficacité d'un blindage métallique face à une onde électromagnétique de fréquence f, on se réfère à la grandeur appelée *épaisseur de peau* δ :

$$\delta = \frac{1}{\sqrt{\sigma \cdot \mu \cdot \pi \cdot f}}$$

où μ et σ sont respectivement la perméabilité magnétique et la conductivité électrique du métal constituant le blindage. Par exemple, pour la fréquence 13,56 MHz, les épaisseurs de peau du cuivre et de l'aluminium sont respectivement de 18 et de 22 µm. Le blindage est

d'autant plus efficace que son épaisseur de métal est grande par rapport à δ. Ainsi, une feuille d'un millimètre d'épaisseur de cuivre ou d'aluminium suffit à bloquer une communication RFID. Des trous ou des fentes sont même possibles dans le blindage, tant que leurs dimensions sont petites par rapport à la longueur d'onde qui est de 22 m dans notre cas. Le blindage électromagnétique est donc une solution efficace avec des moyens simples.

Lorsque des modifications importantes de la solution RFID sont envisageables, d'autres solutions sont aussi possibles. L'ajout d'une pile à l'étiquette permet par exemple de ne plus être limité à des algorithmes qui consomment peu d'énergie. Ainsi, il serait possible d'utiliser des primitives cryptographiques connues publiquement pour leur bon niveau de sécurité. Il existe des piles qui s'intègrent très bien aux cartes RFID de format carte bancaire [27]. Cette solution revient donc à déplacer ces étiquettes dans la catégorie des étiquettes actives et possèdent le même inconvénient : le coût important. En effet, une étiquette active coûte plus de \$25 alors qu'une étiquette passive coûte entre \$0.07 et \$5 selon la fréquence qu'elle utilise, la quantité de mémoire et les matériaux utilisés.

Une alternative de plus en plus attrayante est d'intégrer les solutions RFID dans des applications pour téléphones intelligents. En effet, la technologie NFC permet à certains de ces appareils d'effectuer des communications RFID. Dans ce cas, le manque d'énergie des étiquettes passives est comblée et un niveau de sécurité satisfaisant peut être atteint. Cependant, cette technologie est encore récente et aucune norme n'existe concernant la sécurité de ses communications.

CHAPITRE 3

ÉTUDE D'ATTAQUES EXISTANTES SUR LA SOLUTION ICLASS DE HID

L'étude de résultats scientifiques existants n'est pas dénuée de sens ou d'intérêt. La reproductibilité des résultats est un des piliers de la méthode scientifique. Elle s'appuie sur la description détaillée des expériences et la mise à disposition de toutes les données utilisées. Ainsi, un résultat peut être confirmé ou infirmé par une tentative de reproduction. Dans le cadre de notre étude, la reproduction partielle ou totale d'attaques possède un autre avantage : elle nous permet de mieux évaluer l'effort requis en termes de coût, de connaissances nécessaires et de temps pour effectuer ces attaques. Nous pouvons ainsi apprécier la viabilité de ces attaques pour un attaquant donné et donc évaluer le risque associé. Ces informations participent ensuite à l'élaboration d'une méthodologie normalisée pour évaluer les solutions RFID.

Lors de nos travaux, notre attention s'est portée sur la solution iClass de HID qui est très utilisée comme système de contrôle d'accès. De plus, au début de nos recherches la sécurité de cette solution n'avait pas encore été mise en défaut. Pour notre étude nous avions besoin d'outils polyvalents comme la carte Proxmark3 ou les dispositifs de la famille OpenPCD. Cependant, aucun de ces outils n'implémentait la norme ISO/IEC 15693 utilisée par la solution iClass à ce moment là. Nous avons donc choisi de l'implémenter sur la carte Proxmark3 que nous avions déjà utilisée auparavant. Cette implémentation s'est faite en parallèle de celle de Garcia *et al.* [6, 7] dont nous avons plus tard reproduit les résultats. De plus, contrairement à eux nous avons décidé de créer un nouveau module pour le FPGA de la Proxmark3 entièrement dédié à la norme ISO/IEC 15693.

Ainsi, dans ce chapitre, nous présentons d'abord notre implémentation de la norme ISO/IEC 15693 sur la carte Proxmark3. Ensuite, nous décrivons notre reproduction de l'attaque de Meriac [21] consistant à récupérer la mémoire du microcontrôleur d'un lecteur iClass afin de cloner les cartes du niveau *Standard Security*. Enfin, nous exposons notre étude des attaques cryptographiques sur la solution iClass, principalement effectuées par Garcia *et al.* [6, 7].

3.1 Implémentation de la norme ISO/IEC 15693 sur la carte Proxmark3

3.1.1 Présentation de la carte Proxmark3

La carte Proxmark3 (voir figure 3.1) est un outil très utile pour étudier les produits utilisant la technologie RFID et qui coûte environ $200. C'est le fruit d'un projet de Jonathan Westhues, qui a rendu publics tous ses fichiers sources, sa documentation ainsi que les données nécessaires à la reproduction de la carte électronique. Une communauté s'est formée pour continuer le développement de cet outil, sans son concepteur, autour du site internet `proxmark.org`. Celui-ci héberge notamment tous les fichiers nécessaires au fonctionnement de la carte ainsi qu'une bonne documentation. La liste et les références des composants de la carte [29] ainsi que ses schémas électroniques [30] sont fournis avec les fichiers.

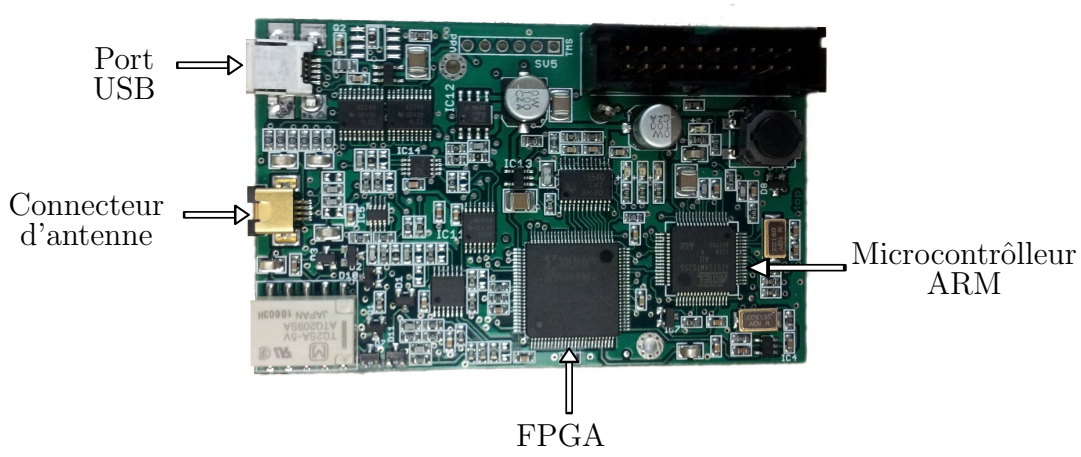

Figure 3.1 La carte Proxmark3 vue de dessus

La Proxmark3 est conçue pour fonctionner aussi bien avec les communications RFID à basse-fréquence (125 et 134 kHz) que celles à haute-fréquence (13,56 MHz). Avec cet outil, il est possible d'espionner une communication et de simuler un lecteur ou une étiquette. Plusieurs travaux de recherches sur la technologie RFID ont utilisé la Proxmark3 et ont participé à son développement [5, 7, 22].

Un schéma fonctionnel simplifié de la Proxmark3 est donné à la figure 3.2. Le connecteur d'antenne possède quatre broches de raccordement. Deux d'entre elles servent à connecter une antenne haute-fréquence (HF), qui ne fait pas partie de la carte. Les chemins d'émission et de réception haute-fréquence sont connectés en parallèle à ces deux broches. Les deux autres broches sont utilisées de la même façon avec une antenne basse-fréquence (BF) et les chemins d'émission et de réception basse-fréquence. La Proxmark3 est conçue pour être utilisée avec

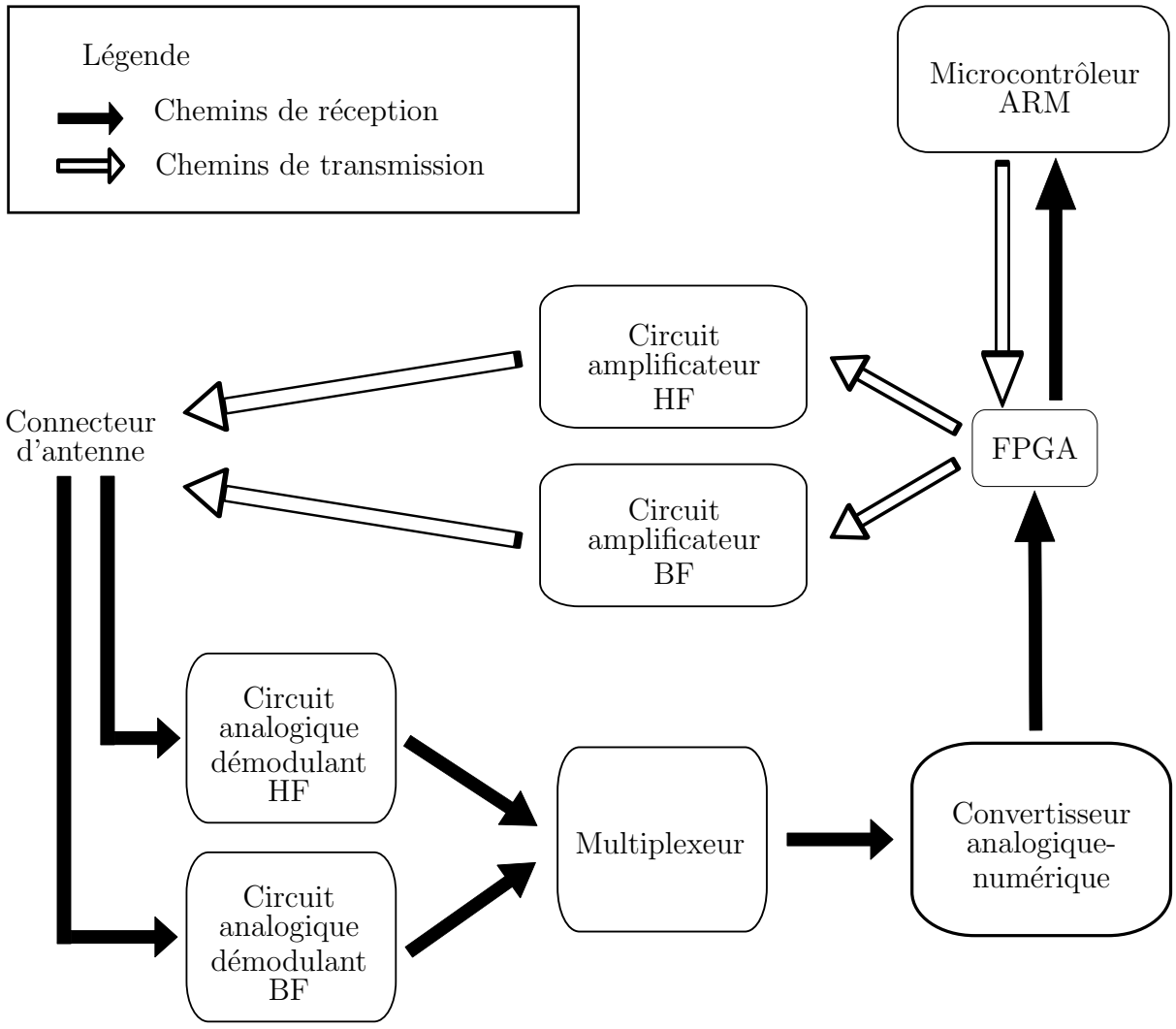

Figure 3.2 Schéma fonctionnel de la Proxmark3

une seule antenne à la fois. La présence d'un seul connecteur d'antenne ne pose donc pas de problème. En fonctionnement, seules deux broches sont connectées à une antenne.

Sur chacun des chemins de réception, un éventuel signal radio-fréquence arrive du connecteur d'antenne puis passe à travers un circuit analogique démodulant qui s'occupe de retirer la porteuse du signal. Le choix entre haute-fréquence et basse-fréquence est effectué par un multiplexeur qui sélectionne la sortie d'un des deux circuits démodulants. Le signal est ensuite numérisé sur 8 bits par le convertisseur analogique-numérique dont la sortie est connectée au FPGA.

Pour la transmission, le FPGA envoie un signal sur l'un des deux circuits amplificateurs qui le relaie ensuite vers le connecteur d'antenne.

Le FPGA est un modèle Spartan-II XC2330 de Xilinx. Il permet d'alléger le traitement du microcontrôleur qui pourrait être débordé par le traitement des signaux, notamment à 13,56 MHz. Le code du FPGA comporte un fichier principal et plusieurs fichiers auxiliaires contenant chacun un module. Le fichier principal implémente la réception de commandes envoyées par le microcontrôleur ARM via une liaison série. Ces commandes déterminent quel module doit être utilisé. Il y a par exemple un module qui s'occupe de recevoir une communication respectant la norme ISO/IEC 14443b, un autre s'occupe de la transmission pour la même norme. Les changements de module sont très rapides et la plupart des cas d'utilisation en nécessitent beaucoup. Dans la commande envoyée par le microcontrôleur, il est aussi possible d'inclure un paramètre qui sera transmis au module sélectionné. Cela permet d'inclure plusieurs modes de fonctionnement dans un même module. Une deuxième liaison série permet au FPGA, ou plus précisément au module sélectionné, d'envoyer le résultat de son traitement au microcontrôleur ARM dans le cas d'une réception et de recevoir des données dans le cas d'une transmission. Il n'y a pas vraiment de règle sur le format des données échangées, qui est conçu par le développeur du module.

Le microcontrôleur ARM est un modèle AT91SAM7S256C d'Amtel. Il implémente le système d'exploitation de la Proxmark3 et gère notamment la connexion USB de la carte. Lorsque celle-ci est reliée à un ordinateur, elle peut être commandée en exécutant son client sur l'ordinateur. Le client permet d'exécuter des fonctions implémentées par le microcontrôleur et réalisant des tâches telles que lire une étiquette ou espionner une communication pour une norme donnée. Ces fonctions utilisent les deux liaisons séries citées ci-dessus pour sélectionner le module FPGA désiré et échanger des données avec le FPGA. Il est aussi possible d'utiliser la Proxmark3 sans client. Dans ce cas, elle ne peut exécuter qu'une seule fonction, prédéfinie dans le code, et déclenchable grâce au bouton présent sur la carte. Pour changer de fonction, il faut donc reprogrammer le microcontrôleur.

La reprogrammation du microcontrôleur et du FPGA s'effectue via la liaison USB. Cette tâche est différente selon le système d'exploitation de l'ordinateur mais très bien documentée.

Lorsque nous avons débuté nos travaux, une partie du code source disponible sur le site `proxmark.org` devait implémenter la norme ISO/IEC 15693, celle utilisée notamment par la solution iClass de HID. Cependant, nous n'avons jamais réussi à obtenir une communication avec des étiquettes de cette norme en utilisant ce code. Nous avons donc choisi d'implémenter nous-même la norme sur la Proxmark3, car nous en avions besoin pour l'étude de la solution iClass (voir sous-section 3.3). Notre implémentation de la norme ISO/IEC 15693 comporte à la fois un nouveau module FPGA et de nouvelles fonctions pour le microcontrôleur ARM. Nous décrivons ici brièvement le comportement de nos ajouts ainsi que les résultats obtenus.

3.1.2 Traitement du signal sur le FPGA

Dans la norme ISO/IEC 15693, les messages envoyés par le lecteur et l'étiquette suivent la même logique. Au début du message, il y a une trame appelée *Start of Frame (SOF)*. S'ensuivent les trames représentant les données à envoyer. Le message se termine par une trame appelée *End of Frame (EOF)*. Cependant, les codages et modulations utilisés par le lecteur et l'étiquette sont différents.

La fréquence de l'onde porteuse est 13,56 MHz et le lecteur utilise une modulation d'amplitude ASK avec un indice de modulation de 10% ou 100%. Le codage des données est implémenté par une modulation de position d'impulsions en mode 1 sur 4 ou 1 sur 256. Dans le mode 1 sur 4, il faut quatre trames pour représenter un octet de donnée alors que dans le mode 1 sur 256 il n'en faut qu'une. La longueur des trames n'est pas la même pour les deux modes. La norme indique que les étiquettes doivent être capables de gérer les deux indices de modulation et les deux modes de codage, qui sont choisis par le lecteur. Cependant, nous n'avons implémenté que le mode de codage 1 sur 4 car c'est celui utilisé par défaut dans la solution iClass. Les différentes trames du mode 1 sur 4 sont illustrées à la figure 3.3. Il s'agit uniquement du signal modulant. Chaque trame de donnée représente deux bits de donnée. Ainsi il y a quatre possibilités qui diffèrent par la position de la « pause » le long de la trame.

De son côté, l'étiquette utilise la modulation de charge pour communiquer avec le lecteur : elle fait varier l'impédance aux bornes de son antenne et donc, par couplage électromagnétique, l'amplitude du signal aux bornes de l'antenne du lecteur. En pratique, l'effet est le même qu'une modulation d'amplitude ASK. Cependant, le signal modulant de l'étiquette est lui même le résultat d'une modulation. Dans le contexte de cette autre modulation, la porteuse est appelée sous-porteuse. Selon la norme ISO/IEC 15693, deux types de modulations peuvent être utilisés avec cette sous-porteuse : une modulation en amplitude ASK avec une fréquence de sous-porteuse de 423,75 kHz ou une modulation en fréquence FSK avec des fréquences de sous-porteuse de 423,75 kHz et 484,28 kHz. Le choix entre ces deux possibilités est fait par le lecteur et dans les deux cas, le codage utilisé est celui de Manchester. Nous n'avons implémenté que la modulation ASK de la sous-porteuse car, une fois de plus, c'est le choix par défaut de la solution iClass. Les différentes trames avec une sous-porteuse modulée en amplitude sont données à la figure 3.4. Une fois encore, il ne s'agit que du signal modulant.

Pour la réception d'un signal, le circuit implémenté par notre module FPGA s'occupe de décoder entièrement le signal qu'il reçoit. Il n'envoie au microcontrôleur ARM que des identifiants représentant les trames reçues, que ce soient celles représentant des données ou celles délimitant les messages(SOF et EOF). En entrée, il obtient du convertisseur analogique-numérique des échantillons sur 8 bits. La fréquence d'échantillonnage de ce dernier est égale

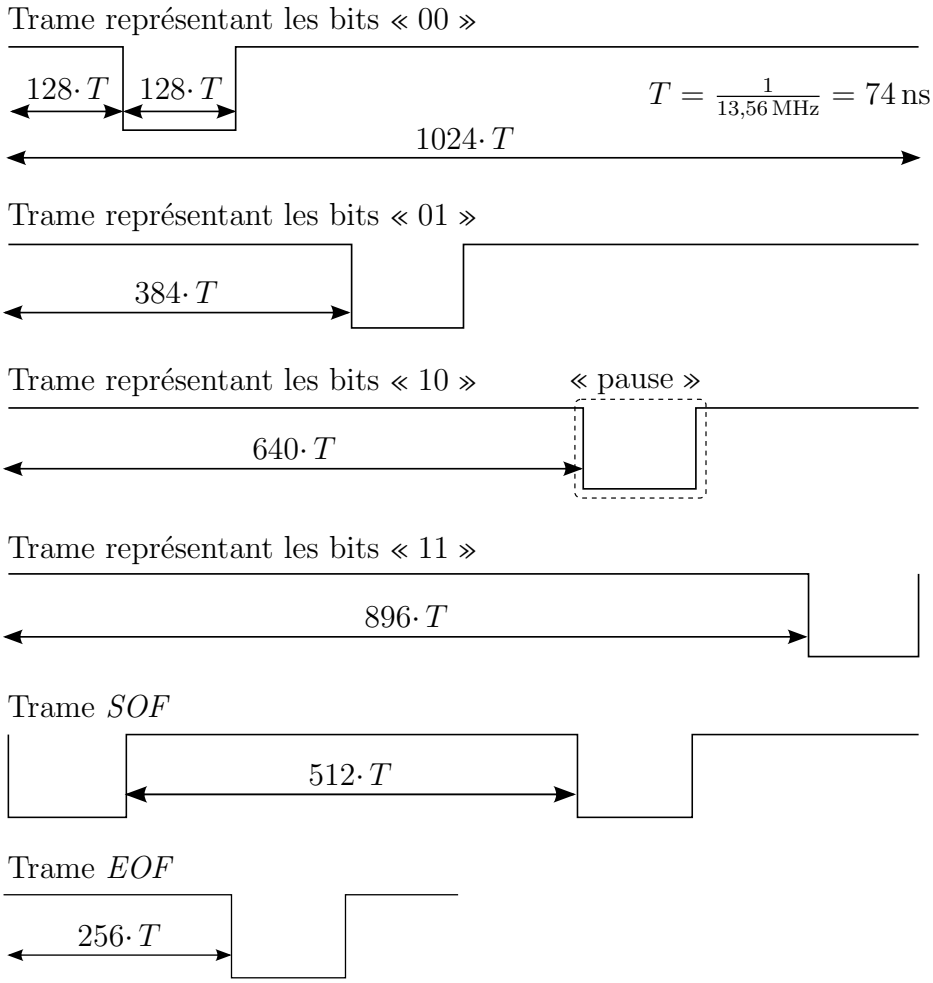

Figure 3.3 Les différentes trames d'un lecteur dans le mode de codage 1 sur 4.

à $\frac{13{,}56\,\mathrm{MHz}}{2} = 6,78\ MHz$. Cela suffit amplement à nos cas d'utilisation et comme l'horloge principale du FPGA provient d'un cristal à 13,56 MHz, toutes les horloges sont des sous-multiples de cette fréquence.

La partie réception implémentée par notre module FPGA comporte deux parties bien distinctes. L'une se charge des messages envoyés par les lecteurs et l'autre se charge de ceux envoyés par les étiquettes. Chacune d'elle reçoit les échantillons du convertisseur analogique-numérique, leur applique un prétraitement puis tente de reconnaître les trames reçues. Le prétraitement permet de nettoyer le signal afin qu'il ressemble plus aux trames épurées théoriques des figures 3.3 et 3.4.

Dans le cas de messages de lecteurs, le prétraitement consiste à déterminer pour chaque groupe de 16 échantillons reçus par le convertisseur analogique-numérique, s'ils représentent un niveau haut ou bas, représenté respectivement par un bit « 1 » ou « 0 » après le pré-

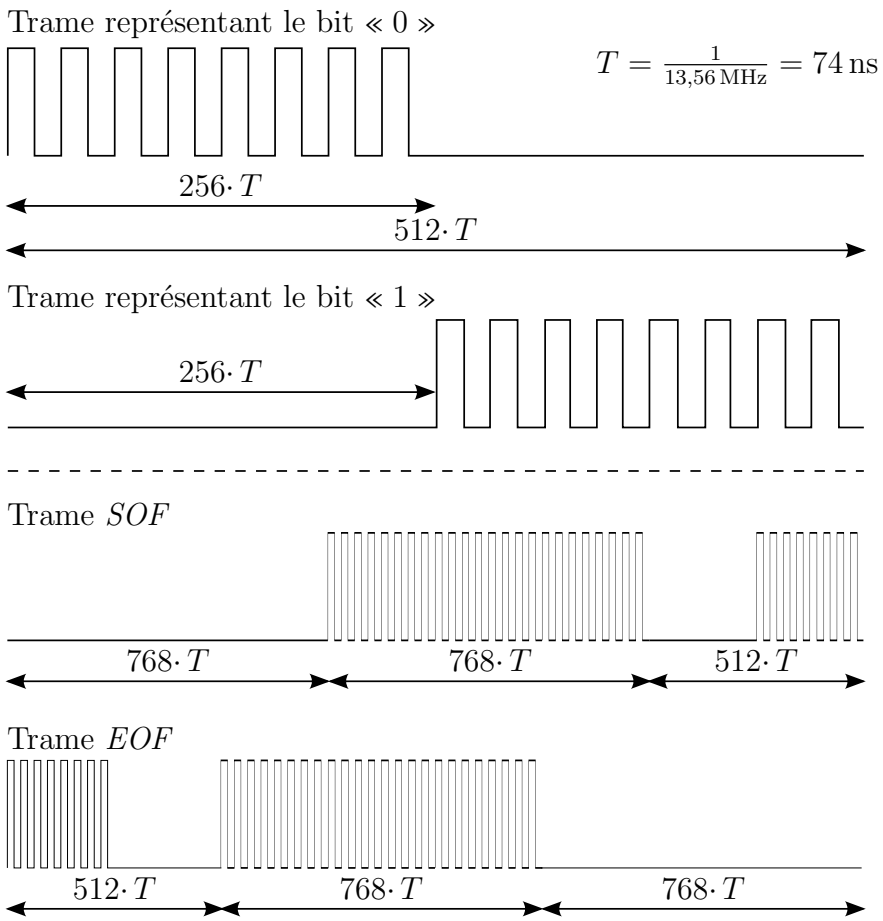

Figure 3.4 Les différentes trames d'une étiquette dans le cas d'une modulation d'amplitude ASK de la sous-porteuse.

traitement. Pour cela, nous faisons la moyenne de ce groupe puis nous la comparons à un seuil déterminé de façon empirique. Cette moyenne permet de réduire l'influence du bruit. Les différentes trames possibles représentées à la figure 3.3 sont ainsi transformées après le prétraitement en séquences de bits telles que données au tableau 3.1. Une taille de groupe d'échantillons égale à 16 permet de représenter une « pause » dans la trame par quatre valeurs après le prétraitement.

En ce qui concerne le prétraitement des messages d'étiquettes, il s'effectue aussi par groupe de 16 échantillons. Ainsi, un groupe représente exactement une période de la sous-porteuse à 423,75 kHz. Dans ce cas, il s'agit de savoir si ce groupe représente la présence de la sous-porteuse ou son absence (voir figure 3.4). Pour ce faire, la différence entre le plus grand et le plus petit échantillon du groupe est comparée à un seuil empirique. Si la différence est au-dessus du seuil alors la sous-porteuse est présente et on représente le groupe de 16 échantillons par un bit « 1 ». Dans le cas contraire, on le représente par un bit « 0 ». Les

Tableau 3.1 Trames d'un lecteur après le prétraitement (dans le mode de codage 1 sur 4).

Trame « 00 »	11110000111111111111111111111111
Trame « 01 »	11111111111100001111111111111111
Trame « 10 »	11111111111111111111000011111111
Trame « 11 »	11111111111111111111111111110000
Trame *SOF*	00001111111111111111000011111111
Trame *EOF*	1111111100001111

différentes trames de l'étiquette représentées à la figure 3.4 sont ainsi transformées après le prétraitement en séquences de bits telles que données au tableau 3.2.

Tableau 3.2 Trames d'une étiquette après le prétraitement (dans le cas d'une modulation d'amplitude ASK de la sous-porteuse).

Trame « 0 »	1111111100000000
Trame « 1 »	0000000011111111
Trame *SOF*	000000000000000000000000111111111111111111111111000000001111111
Trame *EOF*	11111111000000001111111111111111111111110000000000000000000000000

Une fois le prétraitement effectué, dans les deux parties du circuit dédiées à la réception, la reconnaissance des trames suit le diagramme d'état de la figure 3.5. Dans l'état d'attente, le circuit recherche la trame *Start of Frame* indiquant le début d'un message. Celle-ci fait passer le circuit dans l'état de réception. Cet état persiste tant que des trames de données sont reçues mais quand la trame *End of Frame* est reconnue, le circuit retourne à l'état d'attente. Pour chaque trame reçue, l'identifiant correspondant est envoyé au microcontrôleur ARM.

Nous avons de plus ajouté une tolérance aux erreurs. En effet, pour la trame *Start of Frame*, le circuit tolère qu'un certain nombre des bits la représentant après le prétraitement soient inversés. Dans l'état de réception, seules les trames de données et la trame *End of Frame* peuvent être reçues. Nous connaissons donc toutes les possibilités puisqu'il n'y a que quatre trames de données différentes pour un lecteur et deux pour une étiquette. Ainsi, nous prenons parmi elles celle qui est la plus proche de la trame effectivement reçue, selon la distance de Hamming, calculée après le prétraitement.

En ce qui concerne la transmission, le circuit implémenté par notre module FPGA reçoit le signal modulant du microcontrôleur ARM. Dans le cas d'une émission en tant qu'étiquette, c'est le signal modulant la sous-porteuse que le circuit reçoit. La sous-porteuse est générée en divisant l'horloge principale de 13,56 MHz par 32. La modulation d'amplitude et la modulation de charge sont ensuite effectuées par de simples portes logiques « ET ».

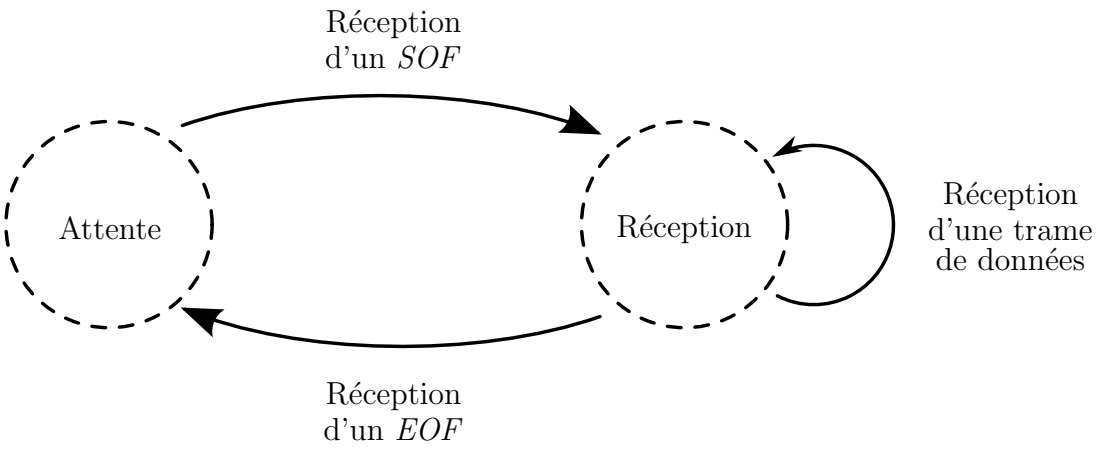

Figure 3.5 Diagramme d'état de la reconnaissance des trames sur le FPGA

Pour une émission en tant que lecteur, le signal reçu du microcontrôleur est directement combiné avec l'horloge principale à l'aide d'une autre porte logique « ET ».

De plus, en mode réception en tant que lecteur, l'onde porteuse à 13,56 MHz continue à être émise pour permettre le fonctionnement des étiquettes interrogées.

Notre implémentation de la norme ISO/IEC 15693 s'appuie sur cinq modes de fonctionnement différents pour notre module FPGA :

- Recevoir en tant qu'étiquette ;
- Transmettre en tant qu'étiquette ;
- Recevoir en tant que lecteur ;
- Transmettre en tant que lecteur ;
- Espionner.

Le mode de fonctionnement est sélectionné par le paramètre que l'on peut passer dans la commande qui choisit le module du FPGA, comme expliqué à la sous-section 3.1.1. Le mode « Espionner » est équivalent aux deux modes de réception en même temps mais sans émission de la porteuse.

3.1.3 La logique de haut niveau sur le microcontrôleur ARM

Les fonctions que nous avons ajoutées sur le microcontrôleur ARM sont inspirées de celles déjà présentes pour d'autres normes. Elles permettent de piloter le circuit implémenté par notre module FPGA en sélectionnant son mode fonctionnement. Elles peuvent aussi stocker les communications effectuées le cas échéant. Afin d'améliorer les performances, le contrôleur

DMA du microcontrôleur est utilisé pour écrire en mémoire ce que le FPGA envoie et lire ce qui doit lui être envoyé.

Quatre des fonctions que nous avons implémentées sont accessibles depuis le client.

hf iclass list : Lister toutes les communications en mémoire.

hf iclass snoop : Espionner une communication.

hf iclass read : Simuler un lecteur.

hf iclass tag : Simuler une étiquette.

Lors de la simulation d'un lecteur ou d'une étiquette, les messages envoyés par la Proxmark3 doivent être prévus à l'avance. Le contenu des messages peut être calculé dynamiquement au moment de la communication mais le déroulement général de celle-ci doit être défini au moment de la programmation du microcontrôleur. Il n'est pas possible de diriger l'échange des messages en temps réel à partir du client car la gestion de la communication USB sur la Proxmark3 induit des délais trop importants dans l'exécution du programme. Cela impose aussi que tous les calculs nécessaires au bon déroulement de la communication doivent être effectués sur la Proxmark3 et ne peuvent être déplacés sur l'ordinateur. Ainsi, tous les algorithmes cryptographiques de la solution iClass, évoqués à la section 3.3, ont dû être implémentés en langage C sur le microcontrôleur ARM.

3.1.4 Performances

Nous avons pu tester notre implémentation de la norme ISO/IEC 15693 en connectant à la Proxmark3 une antenne PCB haute-fréquence achetée sur le site `proxmark3.com` pour environ $20. Nous avons ainsi été en mesure de parfaitement simuler un lecteur ou une étiquette iClass. L'espionnage d'une communication est aussi fonctionnelle. De plus, cette implémentation nous a permis de mener à bien plusieurs de nos travaux suivants (voir sections 3.3, 4.2 et sous-section 4.1.3).

Cependant, il faut noter que la complexité de notre module FPGA, et notamment la présence d'une gestion des erreurs, a considérablement augmenté la taille du circuit à implémenter. En conséquence, il est nécessaire de supprimer les autres modules du FPGA lorsque l'on veut utiliser le nôtre. Une simple reprogrammation permet de les rétablir.

3.2 L'attaque de Milosch Meriac

Cette attaque consiste principalement à récupérer le micrologiciel du microcontrôleur d'un lecteur iClass. Sa conséquence immédiate est de rendre possible le clonage des cartes iClass du niveau *Standard Security*, comme expliqué dans la sous-section 2.2.2. La reproduction de

ce travail est d'autant plus intéressante qu'elle permet de récupérer la clé maître et la clé de chiffrement 3DES, exclues du rapport technique par l'auteur. Or, seule la possession de la clé maître permet de confirmer ces résultats.

Pour commencer, nous avons commandé le matériel nécessaire à la reproduction des travaux de Meriac [21] :

- un lot de dix lecteurs HID iClass RW400 ;
- un câble FTDI TTL-232R-5V-WE ;
- un PICkit2 de Microchip ;
- deux lecteurs HID Omnikey (5321 et 6321).

Le tout a couté environ $600 mais nous aurions pu nous contenter de seulement deux lecteurs iClass et d'un seul lecteur Omnikey. Il est bien sûr nécessaire de posséder au moins une carte iClass.

Dans un premier temps, nous avons vérifié à l'aide du PICkit2 et de son logiciel que les connecteurs à l'arrière du boîtier correspondaient bien aux connecteurs ICSP d'un microcontrôleur PIC18F452. Comme cela était précisé dans le rapport technique [21], nous avons observé que deux de ces connecteurs avaient été intervertis. La mémoire du PIC était bien protégée en lecture et en écriture sur tous les lecteurs. Ensuite, nous avons récupéré les fichiers sources du projet original, fournis par Meriac sur le site `www.openpcd.org`. Parmi eux se trouve notamment le projet de l'application *MicrochipICD*, développée avec C++ Builder. Cette application permet d'utiliser le câble FTDI TTL-232R-5V-WE pour émuler un programmateur de PIC. Le but est d'envoyer des commandes décrites dans les spécifications de programmation de Microchip [23] mais inaccessibles avec le PICkit2 et son logiciel. Ces commandes permettent d'effacer individuellement les différents blocs de mémoire du PIC. Cela a aussi pour effet de supprimer les protections en lecture et en écriture des blocs ciblés. L'application est ensuite utilisée pour écrire un nouveau programme dans ces blocs. Deux programmes peuvent être utilisés, *dumper* ou *dumper-eeprom*. Le premier, lorsqu'il est exécuté par le PIC, lit tout le contenu de la mémoire flash et l'envoie par son port série UART. Le second effectue la même chose mais pour la mémoire EEPROM. Voici les étapes suivies par Meriac pour obtenir tout le contenu de la mémoire du PIC :

1. Effacer le premier bloc de mémoire flash du PIC d'un lecteur RW400.
2. Écrire le programme *dumper* au début de ce bloc.
3. Obtenir les données transmises par le PIC lorsqu'il est redémarré.
4. Effacer de nouveau le premier bloc mémoire flash du PIC du même lecteur RW400.
5. Écrire le programme *dumper-eeprom* au début de ce bloc.
6. Obtenir les données transmises par le PIC lorsqu'il est redémarré.

7. Effacer tous les blocs de mémoire flash sauf le premier du PIC d'un **autre** lecteur RW400.
8. Écrire le programme *dumper* à la fin du dernier bloc de mémoire flash effacé.
9. Obtenir les données transmises par le PIC lorsqu'il est redémarré.
10. Combiner les données obtenues aux étapes 3,6 et 9 pour reformer l'intégralité de la mémoire du PIC.

Plusieurs remarques sont à faire concernant la reproduction de ces étapes. Les étapes 1,2,4,5,7 et 8 sont effectuées avec l'application *MicrochipICD* mais aucune information n'est donnée sur le fonctionnement de l'interface graphique. Une étude du code source est nécessaire pour comprendre le fonctionnement de tous les boutons de l'interface. Il est même indispensable de modifier la valeur d'une variable à l'étape 8 pour définir l'adresse mémoire à laquelle le programme *dumper* va être écrit. De la même façon, la correspondance entre les fils du câble FTDI et les connecteurs du PIC est donnée dans le code source. Aux étapes 3,6 et 9, les paramètres de la communication série sont donnés dans le code source des programmes *dumper* et *dumper-eeprom*. Par défaut la communication se fait à 115 200 baud mais nous obtenions trop d'erreur à cette vitesse et nous l'avons baissée à 9 600 baud. Pour cela, nous avons modifié le code source de ces programmes puis nous les avons recompilés. Enfin, nous avons copié le code assembleur obtenu dans le code source de l'application *MicrochipICD*. Pour la réception de la communication série, nous avons utilisé le câble FTDI ainsi que le programme Putty.

Une fois la mémoire du PIC reconstituée grâce à la librairie *Python library for IntelHEX*, nous avons pu identifier les deux clés indiquées par Meriac. Avant de pouvoir être utilisées avec un lecteur Omnikey, ces clés doivent être permutées en suivant les instructions du constructeur HID Global [10]. Il est possible de le faire avec un script en PHP qui est fourni avec les fichiers sources du projet. Après avoir téléchargé, depuis le site de HID Global, les pilotes et le kit de développement des lecteurs Omnikey, nous nous sommes intéressés au programme *CopyClass*, également présent avec les fichiers sources du projet. Celui-ci nous a permis de lire le contenu des cartes HID iClass en fournissant la clé maître, mais pas de le déchiffrer. Il y avait pourtant une case à cocher dans l'interface graphique du programme pour activer le déchiffrement mais elle n'était pas accessible, elle était grisée. Il est nécessaire d'ajouter une instruction dans le code pour activer cette case. Il faut aussi entrer la clé 3DES de chiffrement directement dans le code source. Une fois ces opérations réalisées, nous avons eu accès au contenu déchiffré des cartes.

Pour cloner des cartes iClass, Meriac rapporte avoir utilisé le programme *ContactlessDemoVC*, fourni dans le kit de développement des lecteurs Omnikey, mais absent de la version disponible au début de notre projet. Ce programme a été supprimé du site de HID Global,

mais il est encore possible de le trouver par une recherche Google. Nous avons tenté de modifier la valeur de certains blocs de l'application 1 des cartes iClass que nous possédions, en utilisant l'application *ContactlessDemoVC* et les commandes décrites dans le rapport technique. La commande d'écriture a nécessité l'utilisation d'une version antérieure du pilote des lecteurs Omnikey, puisque HID global l'avait modifiée (Meriac, courriel, 28 novembre 2011). L'ancienne version du pilote Omnikey est disponible sur le site `www.proxmark.org`.

Finalement, nous avons réussi à reproduire le travail de Meriac en moins de deux semaines effectives, avec quelques connaissances des microcontrôleurs PIC et de bonnes bases en C++. L'existence de cette attaque présente un risque très important pour tous les clients de HID Global dans le monde, qui utilisent la solution iClass dans le niveau *Standard Security*. En effet, dans le cadre du contrôle d'accès, la possibilité de pouvoir reproduire les cartes d'accès rend la solution inutile puisque la possession de la carte n'est plus un critère d'authentification.

Nous rappelons ici les principales étapes permettant de cloner une carte iClass du niveau *Standard Security* :

1. Obtenir la clé maître d'authentification depuis la mémoire du microcontrôleur d'un lecteur iClass dans le niveau *Standard Security*.
2. Utiliser cette clé et un lecteur Omnikey pour lire le contenu de la carte ciblée (avec le programme *CopyClass* par exemple).
3. Écrire les données de la carte ciblée sur une autre carte iClass grâce à l'application *ContactlessDemoVC*.

3.3 Les attaques cryptographiques sur iClass

Comme expliqué dans la sous-section 2.2.2, les travaux de Garcia *et al.* [6, 7] ont révélé successivement les différents algorithmes de la solution iClass :

- l'algorithme de diversification de clé du niveau *Standard Security* ;
- l'algorithme d'authentification ;
- les modifications de la diversification de clé utilisées dans le niveau *Elite*.

Les différentes attaques proposées dans ces travaux reposent essentiellement sur ces algorithmes. Il est donc très important que ceux-ci soient exacts. Dans leur second article [7], les auteurs mentionnent les travaux d'une autre équipe [17]. Celle-ci avait tenté de reconstruire l'algorithme d'authentification, à partir de l'observation des différentes couches de la puce électronique d'une carte iClass, comme cela avait été fait pour la carte Mifare Classic (voir sous-section 2.2.1). Cependant, Garcia *et al.* affirment dans leur article que les résultats de Kim *et al.* sont erronés puisqu'ils diffèrent des leurs.

Selon nous, la seule méthode objective pour déterminer la bonne version de l'algorithme était de tester les deux versions. Nous avons commencé par implémenter l'algorithme d'authentification de Garcia *et al.*. Cependant, nous n'avons pas réussi à reproduire les exemples donnés dans leur article. De ce fait, nous les avons joints par courriel, en leur expliquant notre situation. En leur fournissant notre implémentation de leur algorithme, ils se sont rendus compte qu'une erreur était présente dans la description de l'algorithme, dans leur article. Une fois cette erreur corrigée, dans l'article comme dans notre code, nous avons pu reproduire leurs exemples.

Afin de vérifier, de manière certaine, l'exactitude de l'algorithme d'authentification de Garcia *et al.*, nous avons voulu le tester lors d'une communication avec une carte ou un lecteur iClass. Nous avons donc aussi implémenté l'algorithme de diversification, déjà révélé dans un article précédent [6]. Une fois ces deux algorithmes intégrés sur la Proxmark3 à notre implémentation de la norme ISO/IEC 15693 (voir section 3.1), nous avons pu attester de l'exactitude des algorithmes décrits par Garcia *et al.*. En effet, ils nous est désormais possible de simuler entièrement un lecteur ou une carte iClass en reproduisant toutes les phases de l'authentification. Nous n'avons pas estimé nécessaire d'implémenter l'algorithme décrit par Kim *et al.* puisque les différences avec celui de Garcia *et al.* étaient apparentes et qu'un seul des deux pouvait être exact. Effectivement, les deux algorithmes ne différaient que par certains facteurs d'une sous-fonction linéaire.

En ce qui concerne les modifications de la diversification de clé pour le niveau *Elite*, nous n'avons pas pu les confirmer puisque nous ne possédions ni lecteur, ni carte iClass opérant dans ce mode.

Selon nous, tout ceci vient renforcer l'importance de la reproduction des résultats par d'autres équipes de recherche. Sans cela, l'erreur dans l'article de Garcia *et al.* [7] n'aurait peut-être pas été découverte puisque l'erreur des auteurs n'était pas dans leur implémentation de l'algorithme mais dans sa retranscription mathématique.

Notre travail montre que maintenant que tous les algorithmes de la solution iClass ont été révélés, il est possible de les implémenter sur un outil comme la Proxmark3. Cela n'a aucun coût, hormis le temps de programmation, et permet de simuler un lecteur ou une carte iClass. Grâce à cela, il est possible de lire une carte et d'obtenir toutes les informations que contient sa première application. Ensuite, cette carte peut être simulée à partir de la Proxmark3 ou encore clonée en écrivant les données d'authentification sur une autre carte. De plus, il n'est pas possible de colmater la brèche comme pour l'attaque de Meriac [21] en changeant le microcontrôleur des lecteurs iClass. Les algorithmes sont connus et Garcia *et al.* ont montré qu'il était possible d'obtenir la clé maître d'un lecteur de niveau *Standard Security* ou *Elite*, en effectuant des communications RFID avec ce lecteur. Ainsi, seul un remplacement complet

de la solution résoudrait les problèmes de sécurité.

CHAPITRE 4

ÉTUDE DES LIMITATIONS PHYSIQUES DE LA COMMUNICATION

La technologie RFID s'appuie à la fois sur les principes de communication radiofréquence et sur ceux de l'induction électromagnétique. Ainsi, les limitations de ces deux domaines s'appliquent aussi aux communications RFID.

À 13,56 MHz, l'étiquette utilise le couplage magnétique pour tirer son énergie de l'onde porteuse émise par un lecteur. Or ce couplage n'est possible que dans la zone de champ proche de l'antenne du lecteur. Le champ proche se caractérise par une distance à l'antenne petite par rapport à $\frac{\lambda}{2\pi} = 3{,}52\,\text{m}$, avec $\lambda = 22{,}12\,\text{m}$ pour la fréquence 13,56 MHz. Cette valeur nous donne donc une borne supérieure non inclue de la distance maximale pour effectuer une communication avec une étiquette RFID. En pratique cependant, cela ne nous dit pas jusqu'à quelle distance nous pourrions augmenter la distance de lecture d'une étiquette avec la Proxmark3, au-delà des quelques centimètres atteints par les lecteurs commerciaux standards.

D'autre part, les cages de Faraday et le blindage électromagnétique sont couramment utilisés pour isoler un périmètre des ondes électromagnétiques. Il est donc cohérent que ce type de protection soit proposé pour se protéger des communications RFID non voulues. Cependant, aucune information n'est donnée quant aux limites de ces protections. Que se passe-t-il, par exemple, lorsque la carte sort légèrement de sa protection ?

Ainsi, dans ce chapitre, nous présentons d'abord notre tentative d'augmentation de la distance de lecture d'une étiquette avec la Proxmark3. Ensuite, nous décrivons notre évaluation des protections commerciales utilisant le blindage électromagnétique.

4.1 Augmentation de la distance de lecture d'une étiquette avec la Proxmark3

Comme nous avons pu le voir dans la section 2.2, de nombreuses attaques connues ont été effectuées à l'aide de la Proxmark3. Nous avons déjà présenté ce puissant outil pour l'étude des solutions RFID ainsi que notre implémentation de la norme ISO/IEC 15693 à la section 3.1. Notre but ici est de trouver un moyen d'augmenter la distance de lecture d'une étiquette avec la Proxmark3. Ce moyen, une fois découvert, doit être facilement reproductible, sans connaissances particulières en radiofréquences ou couplage magnétique. Contrairement aux travaux présentés à la section 2.3, nous attachons plus d'importance à la facilité de reproduction qu'à un budget de réalisation le plus petit possible. Nous présentons maintenant le cheminement suivi jusque là, l'état actuel des travaux et leurs performances, ainsi que les

travaux futurs sur ce projet.

4.1.1 Une Proxmark3 et deux antennes

Dans notre utilisation normale de la Proxmark3, nous utilisons une antenne PCB haute-fréquence achetée sur le site `proxmark3.com` pour environ $20. Cette antenne est directement reliée à la Proxmark3 par son connecteur d'antenne et sert aussi bien en réception qu'en émission. Si nous voulons augmenter la distance de lecture d'une étiquette, il faut changer d'antenne et augmenter le courant qui la parcourt grâce à un amplificateur de puissance, comme l'ont fait [19]. Dans ce cas, l'amplificateur va isoler l'antenne de la Proxmark3. Il ne sera donc plus possible de lire les réponses de l'étiquette aux bornes de la Proxmark3 qui servent à l'émission. Ainsi, il nous faut deux bornes de réception, différentes des bornes d'émission. Or, il se trouve que cet outil possède nativement deux chemins de réception et deux chemins d'émission mais l'un de ceux-là est utilisé pour les communications RFID basse-fréquence [30].

Après étude des circuits dédiés aux basses fréquences, il s'avère que seul le chemin de réception est vraiment personnalisé pour ces fréquences. En effet, le circuit analogique de démodulation présent sur le chemin de réception ne peut pas être utilisé en haute-fréquence. Les chemins de transmission quant à eux, ne diffèrent que par la valeur des capacités permettant l'adaptation d'impédance avec les antennes. Ces capacités peuvent très bien être compensées en aval de la Proxmark3, si besoin est. Ainsi, notre système pourra utiliser le chemin de réception dédié aux hautes fréquences et le chemin d'émission dédié aux basses fréquences.

Ce choix implique une modification du code du FPGA. En effet, c'est ce dernier qui décide par où doit transiter le signal d'émission pour aller jusqu'au connecteur d'antenne. Cette décision dépend uniquement du mode de fonctionnement sélectionné par le microcontrôleur ARM (voir section 3.1). Plutôt que de créer un nouveau mode de fonctionnement, nous avons décidé de gérer ce cas grâce à un paramètre générique pour notre module VHDL qui implémente la norme ISO/IEC 15693. Cette solution est donc applicable à tous les autres modules FPGA existants pour la Proxmark3. Il suffit de tester la valeur du paramètre générique et de décider en conséquence sur quel chemin d'émission le signal va être envoyé. Cependant, il faut modifier la valeur de ce paramètre dans le code du FPGA et reprogrammer la Proxmark3 si l'on veut passer d'une version à l'autre.

Une fois les chemins de réception et de transmission choisis, sur la Proxmark3, il reste à décider comment acheminer la réponse de l'étiquette jusqu'à la Proxmark3. Pour cela, nous avons envisagé deux possibilités qui sont illustrées aux figures 4.1 et 4.2 :

Une seule antenne. L'utilisation d'une antenne unique nécessite un moyen de prélever la

valeur de la tension à ses bornes et de l'amener aux bornes de réception haute-fréquence de la Proxmark3. Cependant, il ne faut pas perturber le signal de l'antenne au risque de perdre de la puissance d'émission. Il est aussi important de ne pas détruire des composants du chemin de réception en amenant une tension trop élevée aux bornes de la Proxmark3. Un dispositif tel que celui utilisé par Kirschenbaum et Wool [19] serait envisageable pour cette configuration. Une solution à une antenne unique est plus mobile que la solution à deux antennes, et convient mieux à une attaque ciblée classique sur une étiquette RFID.

Deux antennes. Avec deux antennes, la situation est simplifiée. Une des antennes ne s'occupe que de l'émission et la tension à ses bornes ne nous intéresse pas. L'autre antenne est chargée de la réception et nous pouvons traiter le signal qu'elle reçoit pour l'adapter à la Proxmark3, sans peur de perdre de la puissance d'émission. De plus, en plaçant les deux antennes de part et d'autre de l'étiquette (voir figure 4.2), on diminue la puissance de la porteuse du signal à l'antenne de réception. Ceci permet d'avoir un meilleur rapport entre l'intensité de la porteuse et celle de la modulation de charge de l'étiquette. Il est vrai que cette configuration ne correspond pas au scénario classique où un attaquant communique avec une étiquette RFID en passant plus ou moins près de sa victime. Cependant, elle convient parfaitement à une attaque systématique en un point fixe sujet à beaucoup de passage, comme un encadrement de porte.

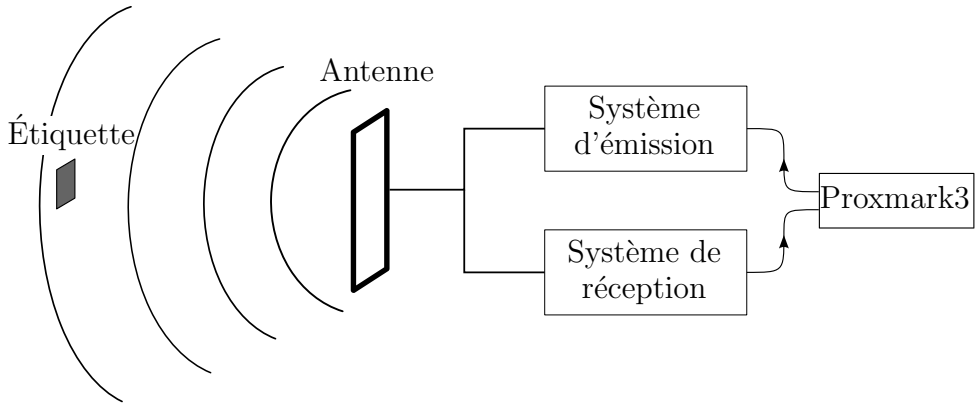

Figure 4.1 Configuration à une seule antenne

À ce stade, il est important de remarquer qu'aussi bien la réalisation de la partie émission de notre système, que la configuration de la Proxmark3, sont complètement indépendantes du choix du nombre d'antennes utilisées.

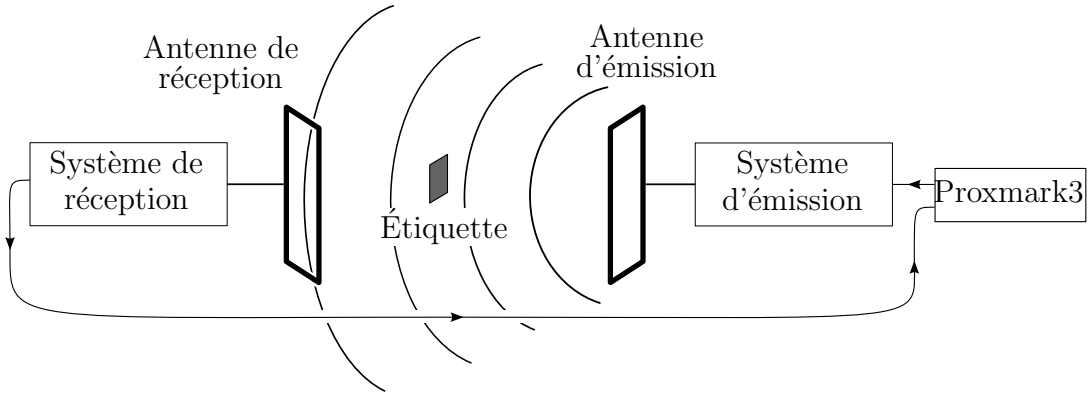

Figure 4.2 Configuration à deux antennes

4.1.2 Réalisation de l'émission

Afin de ne pas multiplier les difficultés lors de la réalisation de notre système, nous avons décidé de ne mettre au point que la partie émission, dans un premier temps. De plus, une fois cette partie réalisée, notre système pourra être utilisé dans une configuration intermédiaire (voir section 4.1.3).

Dans ce projet, nous voulions notamment démontrer qu'il était possible d'interfacer la Proxmark3 avec du matériel utilisé classiquement en communication radiofréquence. Ainsi, l'existence de notre système pourrait pousser des experts de ce domaine à creuser la même piste. C'est pour ces raisons que nous avons décidé de commander du matériel radiofréquence à impédance normalisée de 50 Ω. Conséquence directe de ce choix, il faut effectuer une adaptation d'impédance à la sortie de la Proxmark3.

La première étape a été de choisir l'amplificateur de puissance. Les caractéristiques que nous recherchions étaient :

Un gain le plus important possible. Cela permet d'avoir une puissance d'émission plus importante et donc potentiellement une distance de communication plus grande. Cependant, il faut faire attention à ce que l'amplificateur n'ajoute pas trop de bruit. Pour cela, le facteur de bruit ne doit pas être trop haut.

Une bande passante contenant la fréquence 13,56 MHz. Cette caractéristique est évidente mais essentielle. De plus, comme cette fréquence n'est pas utilisée habituellement à une puissance importante, les amplificateurs de puissance qui conviennent ont une bande passante très large et le choix est moins important que pour des fréquences supérieures à 100 MHz.

Une bonne isolation entre l'entrée et la sortie. Elle assure que les fortes puissances

présentes en aval de l'amplificateur n'endommageront pas les circuits logiques en amont, plus fragiles.

Entrée et sortie en connecteurs coaxiaux. Ce choix permet une plus grande modularité du système global par rapport à un amplificateur qu'il faudrait souder sur un circuit imprimé.

Après quelques recherches, nous nous sommes arrêtés sur le modèle LZY-22+ de la société Mini-Circuits. Ses caractéristiques semblaient convenir à nos attentes (voir tableau 4.1). De plus, cet amplificateur possède des avantages auxquels nous n'avions pas pensé. Il peut être fourni avec un dissipateur de chaleur et un ventilateur qui permettent d'éviter une surchauffe (voir figure 4.3). Il est de plus très robuste car il s'arrête automatiquement s'il y a un risque de surchauffe et il supporte les erreurs d'adaptation d'impédance ou encore les câbles endommagés, coupés, sans risques pour lui et le matériel en amont. Enfin, il peut être allumé et éteint en appliquant ou pas une tension continue sur deux de ses bornes, sans toucher à sa tension d'alimentation. Il a d'ailleurs besoin d'une alimentation de 24 V pouvant fournir jusqu'à 6 A.

Tableau 4.1 Caractéristiques de l'amplificateur de puissance LSY-22+

Bande passante	0,1-200 MHz
Gain typique	43 dB
Isolation	70 dB
Connecteurs	SMA
Alimentation	24 V, 6 A

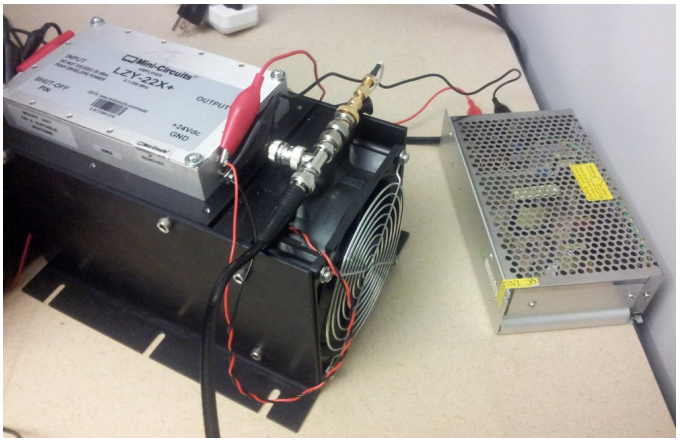

Figure 4.3 Photographie de l'amplificateur LZY-22+ avec son dissipateur de chaleur, son ventilateur et son alimentation

Une fois l'amplificateur de puissance obtenu, il a fallu s'occuper de l'adaptation d'impédance entre la Proxmark3 et lui. Le problème principal est que l'impédance de sortie de la Proxmark3 est complexe mais inconnue et difficilement mesurable avec le matériel que nous avions. Dans un premier temps, nous avons décidé de faire un calcul théorique simplifié de l'impédance, à partir des schémas électroniques de la Proxmark3 [30].

Pour notre calcul, nous négligeons tout le chemin de réception basse-fréquence car celui-ci va être court-circuité lors de la connexion à l'amplificateur de puissance. En effet, il sera connecté au blindage du câble coaxial SMA et donc mis à la masse via le boîtier de l'amplificateur. Après consultation de la liste des composants de la Proxmark3 [29], nous avons ramené son impédance de sortie simplifiée à la représentation de la figure 4.4. Cette représentation prend notamment en compte l'impédance capacitive de sortie de 8 pF de chacun des tampons qui génèrent le courant du signal d'émission.

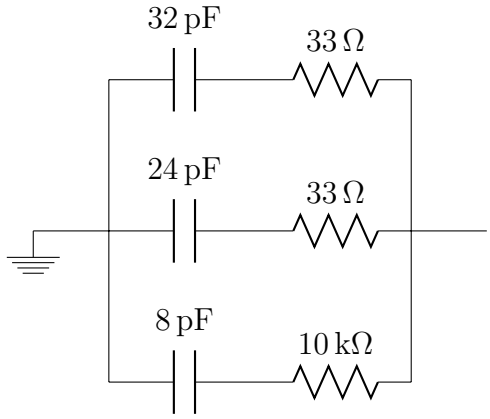

Figure 4.4 Représentation simplifiée de l'impédance de sortie de la Proxmark3

L'impédance de sortie simplifiée est donc :

$$Z_{OUT} = 21 - 208j\ \Omega$$

Ensuite, en utilisant une abaque de Smith, nous avons déterminé théoriquement les composants, et leurs valeurs, nécessaires pour faire l'adaptation d'impédance. Le circuit obtenu est donné à la figure 4.5. Il permet de ramener l'impédance Z_{OUT} à une valeur de $Z_{adapt} = 61 - 2j\ \Omega$. Celle-ci est relativement proche de 50 Ω et sa valeur imaginaire très faible devrait réduire le déphasage au minimum. Dans les faits, nos inductances en parallèle et en série ont des valeurs légèrement différentes qui sont respectivement de 6 µH et 4 µH.

Chacune de ces valeurs est en fait le résultat de la mise en série de deux ou trois inductances.

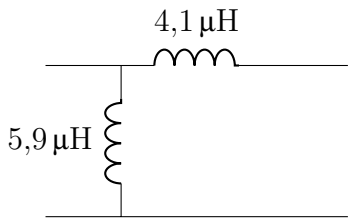

Figure 4.5 Circuit d'adaptation d'impédance

Nous avons soudé les inductances sur un circuit imprimé pré-percé possédant un plan de masse sur l'une des faces. Il faut noter ici que l'utilisation d'une plaquette de prototypage n'est pas possible pour effectuer les tests. En effet, à la fréquence de 13,56 MHz, les capacités parasites des plaquettes de prototypage ainsi que les pattes non coupées des composants ont un effet désastreux sur la qualité du signal.

Afin de vérifier la qualité de l'adaptation d'impédance, nous avons connecté en sortie de l'amplificateur deux résistances de puissance (40 W) de 100 Ω en parallèle. Elles représentent une charge idéale de 50 Ω pour l'amplificateur. Nous avons aussi connecté le circuit d'adaptation entre la Proxmark3 et l'amplificateur. En émettant uniquement l'onde porteuse à 13,56 MHz avec la Proxmark3, nous avons mesuré une tension efficace $V_{RMS} = 37{,}1$ V aux bornes des résistances. La puissance à la sortie de l'amplificateur radiofréquence est donc :

$$P = \frac{V_{RMS}^2}{R} = 27{,}5\,\mathrm{W}$$

Cette valeur est tout à fait satisfaisante et nous avons donc décidé de conserver ce circuit d'adaptation. De plus, le signal ne présentait pas de distorsion importante à l'oscilloscope.

La figure 4.6 montre notre circuit d'adaptation ainsi que ses deux connecteurs. Pour le relier à la Proxmark3, nous avons utilisé un câble Hirose, fourni avec les antennes PCB du site `proxmark3.com`. Nous avons ouvert ce câble afin de séparer les fils correspondant à l'émission et à la réception. Ceux qui servent à l'émission ont été directement soudés sur le circuit d'adaptation, en prenant soin de les torsader afin de réduire les interférences. Nous avons aussi pris un câble SMA que nous avons coupé et soudé à l'autre extrémité du circuit. Il sert à faire la connexion avec l'amplificateur.

Pour l'antenne, nous voulions une impédance de 50 Ω et une taille relativement grande : 0,4x0,4 m est idéale d'après les travaux de Kfir et Wool [16]. Nous avons aussi pensé à construire notre propre antenne mais l'adaptation des antennes cadres est difficile et minutieuse. Cela ne correspondait pas à notre volonté d'une reproductibilité facile de nos travaux. Une fois encore, la fréquence de 13,56 MHz s'est révélée être une contrainte significative.

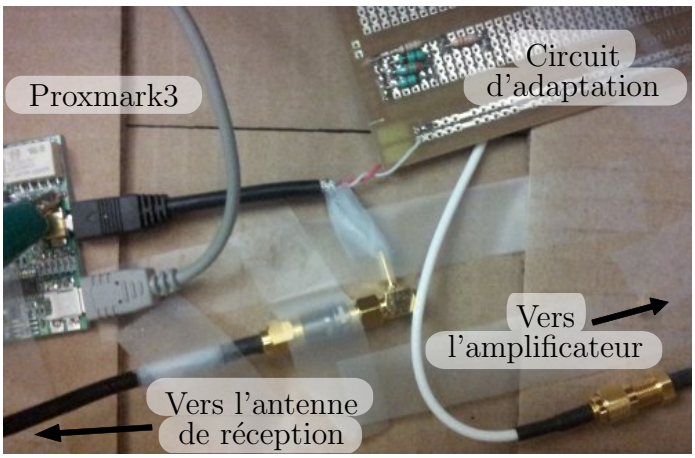

Figure 4.6 Photographie du circuit d'adaptation avec ses connecteurs

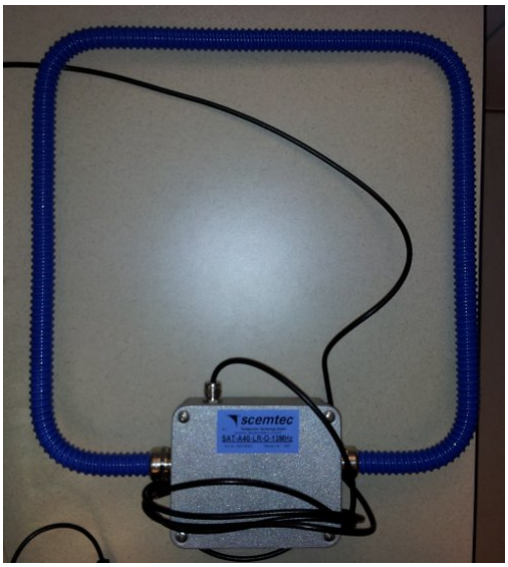

Figure 4.7 Photographie de l'antenne

Cependant, nous avons trouvé une antenne avec toutes les caractéristiques voulues chez la société Scemtec : l'antenne SAT-A40-LR-O (voir figure 4.7). Les dimensions sont exactement celles recommandées par Kfir et Wool.

Le seul point négatif de cette antenne est que la puissance maximale qu'elle accepte en entrée est 7,5 W, d'après un vendeur de la société. Cependant, nous avons soupçonné que cette réponse était uniquement due au fait que le lecteur le plus puissant que Scemtec commercialise avec cette antenne a une puissance maximale de sortie de 7,5 W. Nos recherches ne nous ayant pas donné d'autre antenne candidate, nous sommes restés sur ce choix.

Cependant, nous voulions un moyen de ne pas endommager l'antenne et de pouvoir tester la puissance maximale qu'elle puisse supporter. Pour cela, nous avons commandé un atténuateur variable chez Mini-Circuits dont la référence est ZX73-2500+. En le branchant entre le circuit d'adaptation et l'amplificateur de puissance, nous pouvons faire varier indirectement la puissance en entrée de l'antenne. Cette variation est contrôlée par l'intermédiaire d'une tension de contrôle appliquée sur deux bornes de l'atténuateur. L'atténuation diminue lorsque la tension de contrôle augmente. Avec ce dernier composant, notre système d'émission est complet (voir figures 4.8 et 4.9) et prêt à être mis à l'épreuve.

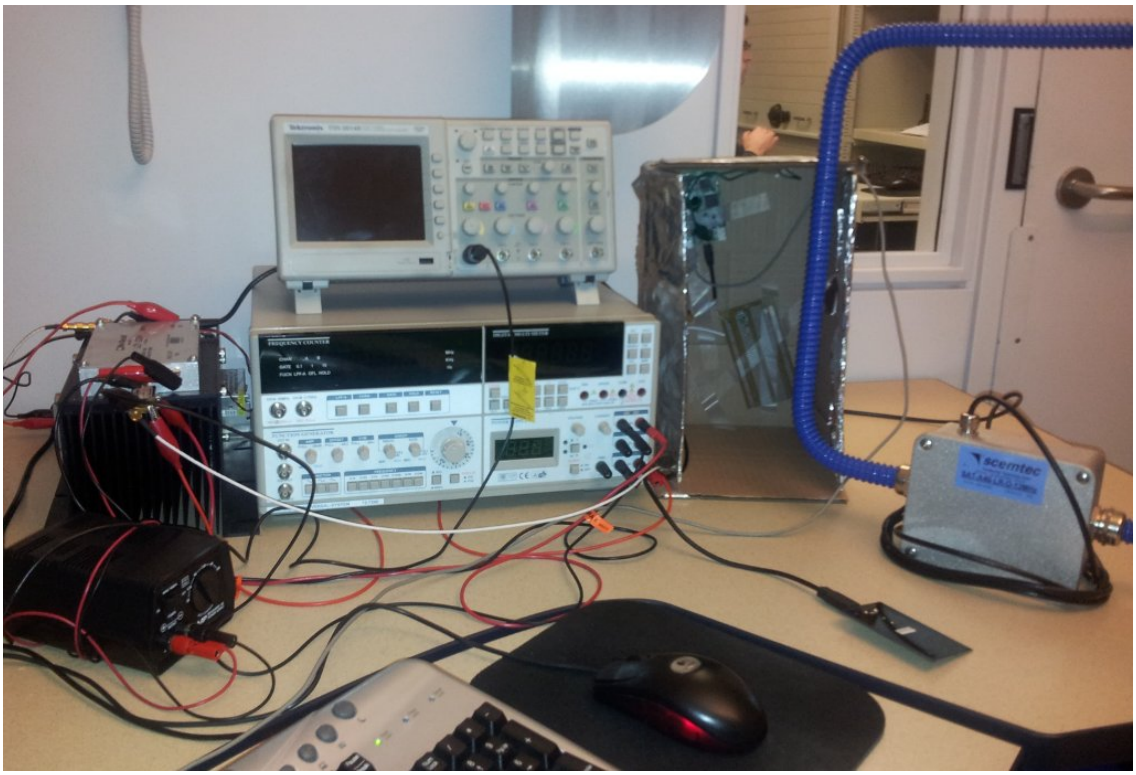

Figure 4.8 Photographie du système d'émission complet.

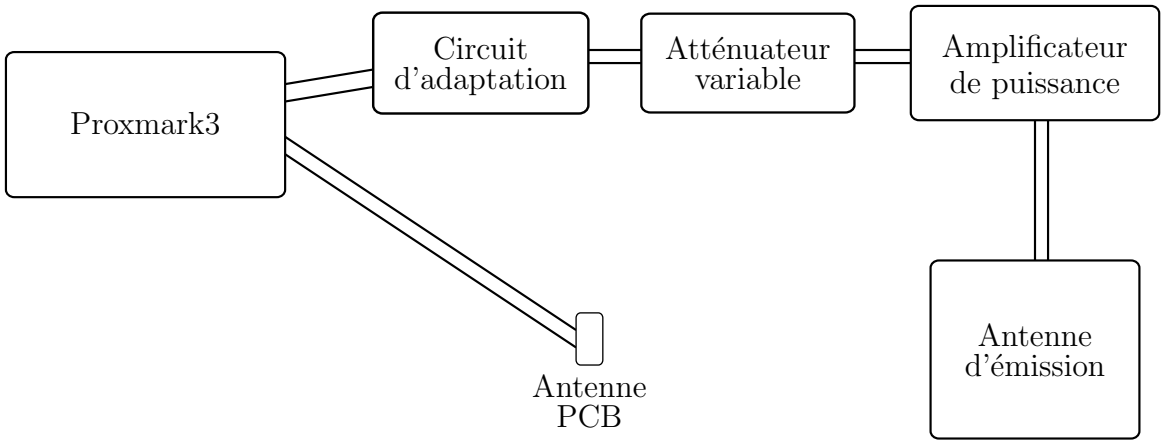

Figure 4.9 Schéma du système d'émission complet sans les différentes alimentations.

4.1.3 Expérience sur la distance d'émission

Cette expérience a pour but d'évaluer la partie émission de notre système. Pour cela, nous utilisons la configuration représentée à la figure 4.10. Le système présenté précédemment est utilisé pour l'émission alors que pour la réception nous utilisons une antenne PCB. La partie réception n'a pas encore été modifiée et elle n'est là que pour attester que l'étiquette soit bien activée et reçoive correctement les messages de la Proxmark3. Ainsi, la distance entre l'antenne PCB et l'étiquette n'est pas importante tant qu'elle permet la communication. Pour cette raison, lorsque nous tentons d'effectuer une communication pendant l'expérience, nous balayons un maximum de positions possibles avec l'antenne PCB. De ce fait, les résultats sont quasiment indépendants de la partie réception de notre système. Pendant cette expérience, nous avons utilisé notre implémentation du protocole iClass pour établir une communication entre la Proxmark3 et une carte iClass. La communication consiste à effectuer toutes les étapes de l'authentification et à lire un bloc mémoire. Si la communication est interrompue, elle est reprise depuis le début jusqu'à en obtenir une complète.

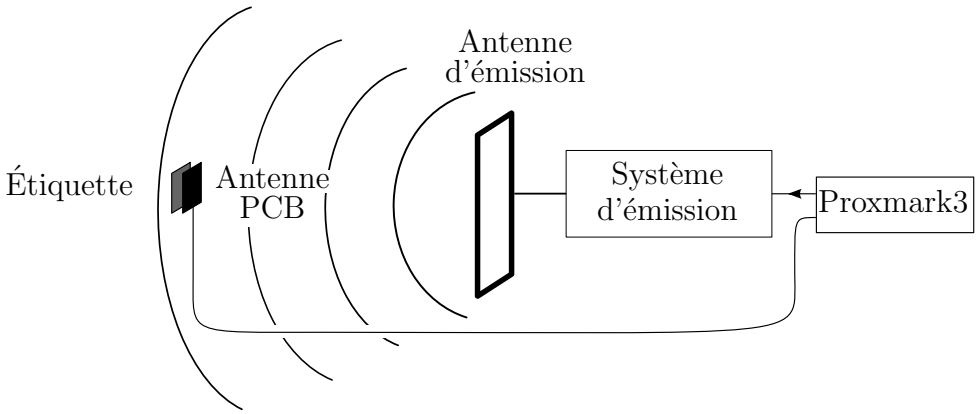

Figure 4.10 Configuration utilisée pour l'expérience

Le protocole expérimental est composé de quatre étapes, répétées pour chaque mesure :

1. Augmenter la tension de contrôle.
2. Mesurer la tension efficace aux bornes de l'antenne.
3. Augmenter la distance entre l'antenne d'émission et l'étiquette jusqu'à ce qu'aucune communication ne soit possible.
4. Mesurer la distance obtenue pour la dernière communication.

Lors de la mesure de la tension efficace aux bornes de l'antenne, la Proxmark3 n'émet que l'onde porteuse à 13,56 MHz. Ceci permet d'avoir une valeur stable, contrairement aux moments où la Proxmark3 émet de véritables messages du protocole iClass. Pour effectuer

cette mesure, nous connectons un « T » à la sortie de l'amplificateur : l'une des sorties va à l'antenne et l'autre est connectée à une sonde d'oscilloscope. Lors des tentatives de communication, le « T » est retiré.

Les résultats de l'expérience sont regroupés dans le tableau 4.2. V_{cont}, $V_{RMS_{ant}}$ et P_{ant} représentent respectivement la tension de contrôle appliquée à l'atténuateur variable, la tension efficace mesurée aux bornes de l'antenne et la puissance fournie à l'antenne. La puissance est calculée selon la formule :

$$P_{ant} = \frac{V_{RMS_{ant}}^2}{50\,\Omega}$$

Tableau 4.2 Résultats de l'expérience sur la distance d'émission

Numéro de la mesure	V_{cont} (en V)	$V_{RMS_{ant}}$ (en V)	P_{ant} (en W)	Distance (en cm)
1	5,0	13,7	3,8	56
2	5,5	14,5	4,2	64
3	6,2	15,5	4,8	66
4	6,6	16,5	5,4	66
5	6,9	17,2	5,9	69
6	7,5	19,0	7,2	75
7	7,7	30,0	18,0	81

Le résultat de la mesure 7 se démarque des autres. Malgré une légère augmentation de V_{cont}, la puissance fournie à l'antenne et la distance de communication ont fortement augmenté. En essayant de renouveler ce résultat, nous sommes arrivés à la conclusion que nous avions court-circuité l'atténuateur variable pour cette mesure. La conséquence a été une atténuation très faible et donc une forte tension aux bornes de l'antenne. Nous avons d'ailleurs pu constater ainsi qu'elle pouvait résister à beaucoup plus de 7,5 W, au moins sur une courte durée. De manière générale, le comportement de l'atténuateur n'a pas été satisfaisant. En effet, nous avons pu remarqué des variations notables de résultat en fonction de la chaleur, et donc de la durée depuis laquelle le système est en marche.

Cependant, ce qui nous importe au final, c'est la relation entre la puissance fournie à l'antenne et la distance de communication (voir figure 4.11). Comme attendu, plus on augmente la puissance d'émission et plus la distance est importante mais avec une relation logarithmique. Grâce à cette expérience, nous savons que nous pouvons activer une étiquette à au moins 81 cm et qu'elle est capable de comprendre les messages de la Proxmark3 et d'y répondre. Nous n'avons pas souhaité augmenter la puissance fournie à l'antenne au-delà des 18 W de la mesure 7 pour deux raisons :

1. Cette distance est suffisante pour nous tant que la partie réception n'est pas au point.

Rien ne sert d'augmenter la distance d'émission si celle de réception est trop faible.

2. Nous ne voulons pas risquer d'endommager l'antenne sachant que le gain ne sera pas très important. En effet, la relation logarithmique de la figure 4.11 laisse penser que nous sommes déjà proches de la limite de notre système.

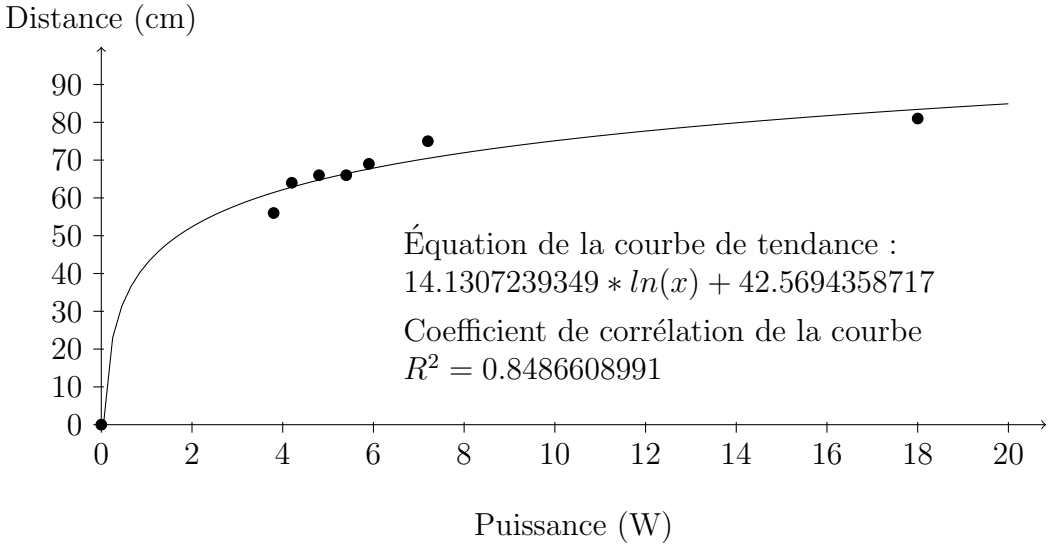

Figure 4.11 Tracé de la distance en fonction de la puissance

La reproduction de ces résultats est très simple, ce que nous souhaitions. Il suffit d'acheter le même équipement, de souder le circuit d'adaptation et de tout brancher ensemble. Ceci est à la portée de toute personne ayant des compétences de base en électronique. Ainsi, bien que la réalisation de ce système nous ait pris environ un an, entre les recherches de matériel, les différents essais infructueux et les délais de livraison atteignant parfois plusieurs mois, nous estimons que sa reproduction ne nécessite pas plus d'une semaine une fois tous les éléments livrés. Un récapitulatif du prix approximatif de chaque élément est présenté au tableau 4.3.

4.2 Évaluation des protections utilisant le blindage électromagnétique

Les protections utilisant le blindage électromagnétique ont été présentées à la section 2.4. Une carte RFID bien en place dans une de ces protections est parfaitement protégée, à moins d'un vice de fabrication majeur. Cependant, qu'en est-il lorsque la carte n'est insérée que partiellement dans la protection ? À partir de quelle longueur de carte à l'extérieur de la protection peut-on l'interroger ? Ces questions sont sans réponse pour l'instant et c'est pourquoi nous avons décidé d'évaluer les performances de ces protections avec le système décrit à la section précédente.

Tableau 4.3 Prix approximatifs des différents éléments de notre système d'émission

Proxmark3	$200
Circuit d'adaptation	$10
Amplificateur de puissance	$1600
Alimentation de l'amplificateur de puissance	$120
Antenne PCB haute-fréquence	$20
Antenne cadre d'émission	$900
Atténuateur variable	$50
Alimentation de l'atténuateur	$200
Coût total	$2900

La partie réception n'est pas nécessaire pour cette évaluation. En effet, une communication établie avec la même configuration (voir figure 4.10) que pour l'expérience de la section précédente est suffisante pour affirmer qu'un risque est présent. Afin de bien montrer la contribution d'une augmentation de puissance en émission, nous effectuons aussi l'expérience avec une Proxmark3 équipée uniquement d'une antenne PCB. C'est donc le cas classique d'utilisation de cet outil avec une antenne PCB qui sert aussi bien à l'émission qu'à la réception. Pour cette expérience, nous utilisons encore une fois notre implémentation du protocole iClass pour établir une communication entre la Proxmark3 et une carte iClass. La communication consiste toujours à effectuer toutes les étapes de l'authentification et à lire un bloc mémoire. Encore une fois, si la communication est interrompue, elle est reprise depuis le début jusqu'à l'obtention d'une complète.

Le protocole expérimental de cette expérience est donc, pour chacun des deux systèmes :

1. Mettre en place la carte RFID dans la protection.
2. Tenter d'établir une communication avec la carte.
3. Sortir peu à peu la carte, jusqu'à ce qu'une communication soit effectuée.
4. Mesurer la longueur de carte dépassant de la protection.

Pour cette expérience, nous nous sommes procurés cinq protections différentes dont les noms et revendeurs sont donnés avec les résultats dans le tableau 4.4 et dont les photographies sont présentées aux figures 4.12, 4.13, 4.14, 4.15, 4.16 et 4.17.

Figure 4.12 Photographie du portefeuille-boîtier fermé

Figure 4.13 Photographie du portefeuille-boîtier ouvert

Figure 4.14 Photographie du porte-badge

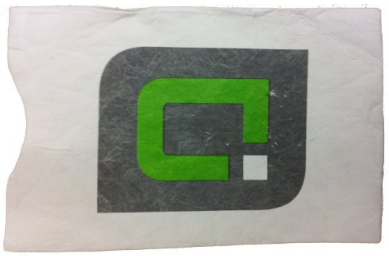

Figure 4.15 Photographie de l'étui à carte

Figure 4.16 Photographie du petit portefeuille

Figure 4.17 Photographie du grand portefeuille

L_{PCB} et L_{SYS} sont les longueurs minimales dont la carte doit dépasser de la protection pour établir une communication avec respectivement le système avec une antenne PCB et notre système avec l'émission améliorée. Notons aussi que, pendant cette expérience, la puissance maximale fournie à l'antenne avec notre système est de 14 W. Les résultats sont obtenus avec l'antenne PCB au plus près de la carte RFID et l'antenne d'émission de notre système à moins de 10 cm.

Tableau 4.4 Résultats de l'évaluation des protections de type blindage électromagnétique

Désignation de la protection	L_{PCB} (mm)	L_{SYS} (mm)	Nom et revendeur de la protection	Prix
Portefeuille-boîtier	∅	∅	Flipside Wallet de Flipside Wallet	$39.95
Porte-badge	∅	∅	Secure Badgeholder Classic de Identity Stronghold	$6.49
Étui à carte	50	12	Secure Sleeve for ID & Payment Cards de Identity Stronghold	$3.99
Petit portefeuille	40	15	RFID Blocking Secure Mini Wallet de Identity Stronghold	$15.95
Grand portefeuille	35	25	RFID Blocking Secure Wallet Bi-Fold 12 de Identity Stronghold	$29.95

Afin de bien comprendre ces résultats, il faut prendre en compte certaines remarques sur chaque protection :

Portefeuille-boîtier et porte-badge : Ces protections maintiennent la carte dans son emplacement de telle façon qu'il est impossible qu'elle sorte sans action de son propriétaire. Il n'est donc pas pertinent d'effectuer des essais en retirant partiellement la carte.

Étui à carte et petit portefeuille : L'insertion de la carte dans ces protections se fait dans le sens de la plus grande dimension de la carte.

Grand portefeuille : L'insertion de la carte dans cette protection se fait dans le sens de la plus petite dimension de la carte.

Petit et grand portefeuilles : Chacun de ces portefeuilles possède plusieurs fentes pour ranger les cartes. Pour les fentes inférieures, lorsque l'on retire la carte, les fentes supérieures participent à bloquer l'onde radiofréquence. Ainsi, les résultats sont donnés pour les fentes les plus hautes qui ne bénéficient pas de ce phénomène.

Notre première conclusion concernant ces résultats est que toutes les protections sont parfaitement efficaces face à notre système, quand la carte est bien à sa place. Cependant, la carte RFID peut sortir partiellement de son emplacement dans l'étui à carte, le petit et

le grand portefeuille. Dans ce cas, chacune de ces protections est vulnérable à partir d'une certaine longueur de sortie.

De plus, l'augmentation de puissance en émission modifie notablement les résultats. Dans le cas de l'étui à carte, la longueur de sortie est environ divisée par quatre. Il n'est donc pas illogique de penser qu'on pourrait encore diminuer ces longueurs en augmentant la puissance d'émission.

En conséquence, nous recommandons plutôt l'usage de protections qui maintiennent parfaitement la carte à son emplacement, telles que le porte-badge ou le portefeuille-boîtier.

CHAPITRE 5

VERS UNE MÉTHODOLOGIE NORMALISÉE

Dans ce chapitre, nous tentons de tirer les grandes lignes de nos travaux ainsi que des travaux précédents que nous avons présentés. À partir de ces principes, nous faisons l'ébauche d'une méthodologie normalisée pour l'évaluation des solutions RFID en sécurité. Cette méthodologie est à double usage :

- Elle permet d'évaluer une solution existante pour mettre à jour ses possibles faiblesses.
- Elle peut aussi servir de cahier des charges partiel pour une nouvelle solution RFID. Ceci permettrait de ne pas renouveler les erreurs faites pour les produits antérieurs.

Nous nous plaçons dans le cas de l'étude d'une solution RFID complètement inconnue utilisant la fréquence 13,56 MHz. Dans le cas d'une solution récemment introduite sur le marché, il est tout à fait possible de se retrouver dans cette situation. Notre première étape est la rétro-ingénierie de la puce d'une étiquette. Cela permet de reconstruire les algorithmes de la solution gardés secrets. Ensuite, nous proposons de découvrir le protocole de communication utilisé par la solution en identifiant la norme qu'elle implémente puis en étudiant des communications espionnées à l'aide d'une Proxmark3. Nous conseillons ensuite une étude statistique des messages de la solution RFID afin de repérer d'éventuelles failles cryptographiques. Enfin, nous recommandons l'étude des conséquences de la capture d'un lecteur de la solution. Cette dernière étape permet d'évaluer les données secrètes récupérables à partir du lecteur et leur champ d'action.

5.1 Étape 1 : Rétro-ingénierie de la puce d'une étiquette

Cette étape est la reproduction des travaux de Nohl et Plötz [25] sur la solution Mifare mais appliquée à notre solution ciblée. Il s'agit donc dans un premier temps d'obtenir la puce de l'étiquette par dissolution de la carte plastique, ou autre contenant, qui l'entoure. Ensuite, il faut photographier à l'aide d'un microscope optique 500x les différentes couches de la puce. Le passage d'une couche à l'autre se fait en ponçant très légèrement la puce. La suite se compose d'une analyse graphique des images permettant de reconstituer les algorithmes utilisés par l'étiquette, à partir des différentes portes logiques identifiées.

Ainsi, cette étape nécessite un microscope optique 500x (environ $300), de bonnes connaissances en analyse graphique automatisée et beaucoup de temps. Cependant, c'est la seule méthode permettant de retrouver un algorithme ne possédant pas d'implémentation logicielle

ou en microcode, comme c'était le cas pour Crypto-1 de la solution Mifare Classic.

5.2 Étape 2 : Détermination du protocole de communication

5.2.1 Quelle est la norme ?

Avant de pouvoir commencer à s'intéresser à la sécurité de la solution ciblée, il est primordial de comprendre le protocole de communication qu'elle utilise. Dans un premier temps, nous nous plaçons dans le cas où nous avons accès à un lecteur et une étiquette en laboratoire. Ainsi, nous pouvons étudier les communications entre eux sans aucune contrainte. En effet, il suffit de placer l'étiquette dans le champ d'action du lecteur pour provoquer une communication.

Il est possible de commencer par s'assurer que l'onde porteuse est bien à la fréquence 13,56 MHz. Pour cela, il existe un moyen très simple ne nécessitant qu'un oscilloscope et une de ses sondes. En effet, en connectant les deux bornes de la sonde entre elles, on crée une antenne capable de capter les ondes à cette fréquence. Ainsi, nous pouvons confirmer sur l'écran de l'oscilloscope la présence d'une onde à 13,56 MHz.

Ensuite, il est nécessaire d'utiliser un outil de bas niveau comme l'USRP mentionné à la sous-section 1.2.2. Il possède une carte-mère et des cartes-filles interchangeables. Pour notre étude, il est essentiel d'utiliser une carte-fille de réception avec une bande-passante comprenant la fréquence 13,56 MHz. De plus, il est recommandé d'utiliser une antenne cadre d'impédance 50 Ω et de fréquence de résonance 13,56 MHz. Une impédance de 50 Ω n'est pas aussi indispensable que dans le cas d'une antenne d'émission mais cela permettra d'avoir un signal plus fort.

La solution RFID étudiée implémente très probablement une des normes RFID existantes, au moins partiellement. Il s'agit donc d'utiliser l'USRP pour reconnaître quelle est cette norme. Ainsi, nous devons numériser une partie de la communication et tenter de la démoduler selon les différentes possibilités décrites par les normes. Si l'une de ces démodulations donne un résultat conforme à la norme associée, alors c'est sûrement la bonne. Il est aussi possible d'essayer de deviner la modulation utilisée. En effet, l'observation du spectre de fréquence de la communication peut indiquer la fréquence des sous-porteuses. De même, l'observation du signal temporel permettra de différencier une modulation en amplitude d'une modulation en fréquence.

Cependant, il faut bien être conscient que la plupart des solutions RFID en application de sécurité utilisent un protocole de haut niveau propriétaire, même si elles respectent une des normes RFID pour les couches inférieures de leurs communications. Nous devons donc découvrir ce protocole de haut niveau par la suite.

Si la communication ne respecte aucune norme, la tâche devient très complexe. Il faut vérifier si certaines démodulations ne donnent pas des schémas qui se répètent et essayer de reconnaître des codages classiques comme celui de Manchester. Cette démarche est très spécifique et n'est pas couverte pas notre méthodologie.

Dans le cas où il n'est pas possible d'avoir le lecteur et l'étiquette en laboratoire, c'est un peu plus fastidieux. Nous pouvons tout de même utiliser l'USRP mais il est nécessaire de l'alimenter par une batterie et le connecter à un ordinateur portable. L'ensemble de ces appareils tient dans une mallette. Comme le signal peut être numérisé et enregistré sur l'ordinateur avant de tenter les démodulations, il suffit de faire une seule acquisition sur le terrain.

5.2.2 Quel est le protocole de haut niveau ?

Une fois la norme identifiée, nous pouvons changer d'outil et utiliser la Proxmark3 qui implémente toutes les normes RFID à la fréquence 13,56 MHz. Même si la norme n'était pas implémentée, il suffirait de le faire comme cela a été notre cas (voir section 3.1). Ainsi, il n'est plus nécessaire de se préoccuper de la modulation et du codage des messages. La Proxmark3 nous donne directement accès aux bits de donnée échangés.

Néanmoins, si aucune autre source d'informations n'est disponible à propos du protocole de haut niveau, sa découverte peut être longue et fastidieuse. Il faut enregistrer un maximum de communications puis les analyser. Les étapes d'une communication sont plus ou moins les mêmes d'une solution RFID à l'autre. On retrouve un processus anti-collision au début, qui permet au lecteur de sélectionner une seule étiquette si plusieurs sont présentes dans son champ d'action. Les étiquettes se présentent au lecteur en donnant un identifiant qui est bien souvent identique d'une communication à l'autre. Ensuite, une authentification a lieu avant de laisser place à des lectures de blocs mémoire de la carte par le lecteur.

Ainsi, en repérant quelles parties de la communication sont constantes, quelles autres changent tout le temps ou encore sont constantes pour une étiquette donnée, on identifie le protocole de haut niveau. À ce stade, nous comprenons les grandes lignes de la communication même si nous ne connaissons pas les algorithmes utilisés pour l'authentification par exemple. Nous pouvons constater que bien souvent, des informations sont disponibles à propos du protocole de haut niveau. En effet, il n'est pas rare que les fabricants expliquent directement sur leur site internet comment fonctionnent leurs protocoles [12, 10].

Si aucune authentification n'est présente dans la communication, l'étude est à toutes fins pratiques terminée. Il suffit de simuler un lecteur face à une étiquette légitime puis une étiquette face à un lecteur légitime pour confirmer que l'on a bien compris le protocole de haut niveau.

5.3 Étape 3 : Étude statistique des messages

La sécurité de tout processus d'authentification repose notamment sur la qualité des sources de nombres pseudo-aléatoires utilisées. C'est d'ailleurs la médiocrité des générateurs de nombres pseudo-aléatoires qui est à la base de la vulnérabilité Mifare 2 décrite à la sous-section 2.2.1. De la même façon, l'absence de générateur pseudo-aléatoire sur les cartes iClass (Vulnérabilité iClass 6) est utilisée pour l'attaque de Garcia *et al.* [7] permettant de récupérer la clé maître du niveau de sécurité *Standard*. Ainsi, il est important d'évaluer ce critère pour notre solution ciblée.

La démarche utilise des étapes simples mais prend un certain temps et de l'espace de stockage informatique. En effet, il faut effectuer un très grand nombre de communications et enregistrer les valeurs correspondant aux défis de l'authentification, repérés à l'étape 2. De plus, il faut prêter une grande attention à tous les paramètres dont peuvent dépendre les générateurs de nombres pseudo-aléatoires et les garder constants, autant que possible, d'une communication à l'autre. Parmi ces paramètres potentiels, nous pouvons citer le temps depuis lequel l'étiquette ou le lecteur est alimenté. C'est celui-ci qui détermine les nombres pseudo-aléatoires générés par la solution Mifare par exemple (voir sous-section 2.2.1). Nous pouvons aussi penser à l'identifiant de l'étiquette, l'heure de la communication ou encore un message envoyé dans la communication précédente. Ce dernier est celui utilisé dans la solution iClass de HID (Vulnérabilité iClass 6).

Une fois toutes ces données collectées, leur analyse peut montrer que ces nombres pseudo-aléatoires ne décrivent pas l'ensemble des possibilités. Si c'est le cas, il est intéressant de connaître les causes de cette diminution d'entropie. Cela peut être tout simplement une mauvaise conception des générateurs pseudo-aléatoires mais aussi une dépendance à l'un des paramètres fixés auparavant. Pour s'en assurer, il faut refaire des communications en ne faisant varier qu'un seul de ces paramètres à chaque fois.

Dans un cas extrême pour la solution RFID, la baisse d'entropie peut rendre possible une attaque de force brute, dans un délai raisonnable, sur l'algorithme d'authentification. Dans tous les cas, cela facilitera les attaques possibles en diminuant le nombre d'opérations qu'elles nécessitent.

L'étude statistique peut aussi permettre de révéler complètement les algorithmes utilisés par la solution ciblée. Un bon exemple de cette situation est le travail de Garcia *et al.* [6], lorsqu'ils ont révélé l'algorithme de diversification de clé du niveau *Standard* de la solution iClass (voir sous-section 2.2.2). De manière générale, ce type d'étude permet de juger la qualité des primitives cryptographiques utilisées par le lecteur et l'étiquette. Les défauts de conception peuvent aussi être mis à la lumière et orienter les recherches de vulnérabilités

dans la bonne direction. On se retrouve alors dans des situations à gérer au cas par cas et pouvant nécessiter de bonnes connaissances en mathématiques et statistiques.

5.4 Étape 4 : Étude des conséquences de la capture d'un lecteur

La quatrième étape est particulièrement importante dans la phase de conception d'une solution RFID pour les applications de sécurité. Il s'agit de déterminer l'impact que pourrait avoir la possession ou le vol d'un des lecteurs RFID par un attaquant. L'attaque de Meriac [21] sur la solution iClass illustre bien ce type de situation. En effet, à partir d'un seul lecteur, l'auteur a rendu possible le clonage de n'importe quelle carte iClass du niveau de sécurité *Standard*, dans le monde entier (Vulnérabilité iClass 1). Par la suite, la rétro-ingénierie de la mémoire du microcontrôleur du lecteur a permis de complètement briser tous les niveaux de sécurité de la solution iClass.

Le premier point à étudier est l'accessibilité à des données secrètes à partir d'un lecteur. Les possibilités sont nombreuses mais l'idée générale est toujours la même : peut-on accéder à la mémoire du lecteur et si oui contient-elle des informations sensibles ? La formulation même de cette question montre que deux pistes de solutions sont possibles pour les fabricants de solutions RFID. Soit ils ne laissent aucune information sensible dans la mémoire du lecteur, soit ils s'assurent qu'elles ne pourront jamais être récupérées. Cependant, le lecteur contiendra forcément une implémentation analogique ou logicielle des algorithmes cryptographiques utilisés. La sécurité de la solution ne devrait donc pas s'appuyer sur leur secret.

Le second point d'intérêt est le champ d'action des données sensibles présentes sur le lecteur. Très concrètement, il s'agit par exemple de déterminer pour une solution de contrôle d'accès si la clé maître contenu dans un lecteur est commune à tous les lecteurs d'un client ou de tous les clients. Ce point est très important car dans le second cas, un attaquant peut obtenir le lecteur d'un petit client avant de s'attaquer à sa véritable cible. La motivation d'un attaquant grandira avec le champ d'action des données sensibles et l'impact d'une attaque aussi.

5.5 Limitation

Cette ébauche de méthodologie se fonde sur les différents travaux qui ont été effectués sur des solutions RFID en application de sécurité. Or, les fabricants de la plupart de ces solutions gardent secret les algorithmes cryptographiques utilisés. Ainsi, une partie de cette méthodologie a pour but de révéler ces algorithmes et se révèlerait complètement inutile dans le cas d'une solution entièrement connue.

5.6 Généralisation

Nous avons mis au point cette méthodologie dans le cadre de l'étude des solutions RFID utilisant une onde porteuse de fréquence 13,56 MHz. Cependant, elle peut se généraliser aux autres fréquences de la technologie RFID, dans le cas où un certain niveau de sécurité est nécessaire. De façon générale, il est possible de l'appliquer à d'autre technologies de communication sans-fil utilisées dans des applications critiques. Le domaine de la santé est un très bon exemple. En effet, de plus en plus de capteurs biométriques sans-fil sont utilisés en médecine. Ces appareils sont très contrôlés pour éviter tout dysfonctionnement accidentel et dangereux pour le patient. Néanmoins, la possibilité d'une attaque volontaire n'est pas toujours envisagée, comme le montre les travaux de Barnaby Jack [18]. En effet, ces travaux démontrent la possibilité de déclencher une décharge électrique fatale sur certains modèles de stimulateurs cardiaques.

CHAPITRE 6

CONCLUSION

Le but de cette recherche était de mettre en avant les risques liés à l'utilisation de solutions RFID en application de sécurité et d'élaborer une ébauche de méthodologie normalisée d'évaluation de ces risques.

Ce chapitre conclue la présentation de nos travaux en rappelant les résultats de chacun de nos objectifs de recherche. Les limitations de certains d'entre-eux sont ensuite abordés, puis les travaux futurs sont exposés.

6.1 Synthèse des travaux

Le premier axe de nos travaux est l'étude d'attaques existantes et englobe trois de nos objectifs de recherche.

1. Nous avons implémenté la norme ISO/IEC 15693 sur la carte Proxmark3. Nous sommes maintenant en mesure d'espionner une communication ou encore de simuler un lecteur ou une étiquette utilisant cette norme.
2. Nous avons entièrement reproduit l'expérience de Meriac [21] et obtenu la totalité de la mémoire du microcontrôleur d'un lecteur iClass. Celle-ci contient notamment la clé d'authentification et la clé de chiffrement utilisées par tous les lecteurs et cartes iClass du niveau *Standard Security*, dans le monde entier. La conséquence directe est la possibilité de cloner n'importe laquelle de ces cartes.
3. Nous avons ensuite confirmé les résultats de Garcia *et al.* [7] concernant les algorithmes cryptographiques du niveau *Standard Security* de la solution iClass. Pour ce faire, nous avons implémenté ces algorithmes sur la carte Proxmark3. Nous sommes donc capables de l'utiliser pour lire le contenu d'une carte iClass ou pour simuler un lecteur ou une étiquette afin d'effectuer une communication complète comprenant la phase d'authentification.

Le deuxième axe de nos recherches consiste à étudier les limitations physiques d'une communication RFID.

4. Nous avons réalisé la partie émission d'un système visant à augmenter la distance de communication entre la carte Proxmark3 et une étiquette RFID. Pour cela, nous

avons notamment utilisé un amplificateur de puissance et une antenne cadre de dimensions 0,4x0,4 m. Les résultats obtenus montrent que notre système permet d'activer une étiquette à au moins 81 cm et qu'elle est capable de comprendre les messages de la Proxmark3 et d'y répondre.

5. Nous avons évalué quelques protections de type blindage électromagnétique disponibles sur le marché. Notre expérience démontre qu'elles sont efficaces lorsque la carte est entièrement insérée dans la protection. Cependant, si la carte dépasse de la protection, il existe une longueur de dépassement à partir de laquelle nous avons été capables de l'interroger. En utilisant le système de la section 4.1, nous avons pu remarquer que cette longueur limite diminue lorsque l'on augmente la puissance d'émission du lecteur. Nous avons notamment réussi à communiquer avec une carte iClass ne dépassant que de 12 mm d'un étui de protection.

Notre dernier axe de recherche est la mise au point d'une méthodologie normalisée d'évaluation des risques des solutions RFID en application de sécurité.

6. À partir des résultats de nos travaux ainsi que ceux existants dans le domaine, nous avons élaboré une méthodologie en quatre étapes. Elle a pour but de guider la recherche de vulnérabilités pour une solution RFID complètement inconnue. Elle pourrait aussi servir de cahier des charges partiel pour un nouveau produit, afin de ne pas répéter les erreurs des solutions précédentes.

6.2 Limitations

Certains de nos résultats sont à nuancer. Nous n'avons pas implémenté la totalité de la norme ISO/IEC 15693. En effet, le mode de codage 1 sur 256 du lecteur et la modulation en fréquence FSK de la sous-porteuse de l'étiquette ne sont pas gérés par notre module FPGA ajouté à la Proxmark3. Cependant, cela n'influence pas les résultats obtenus puisque la solution iClass ne les utilise pas.

En ce qui concerne les résultats de Garcia *et al.* [7] sur les algorithmes cryptographiques de la solution iClass, nous n'avons pas pu vérifier ceux du niveau *High Security* puisque nous n'avions ni cartes, ni lecteurs de ce niveau.

Enfin, l'activation de l'étiquette à 81 cm a été réalisé avec une carte iClass, qui implémente la norme ISO/IEC 15693. Nous n'avons pas effectué d'expérience avec des étiquettes suivant d'autres normes.

6.3 Travaux futurs

Le domaine de la sécurité RFID est appelé à prendre beaucoup d'ampleur au cours des prochaines années. Nous avons donc identifié plusieurs pistes de travaux futurs pour lesquels le présent mémoire pourrait servir de base. La suite immédiate de nos travaux est la réalisation de la partie réception de notre système visant à augmenter la distance de communication entre la carte Proxmark3 et une étiquette RFID. L'idéal serait de réaliser les deux configurations différentes, à une antenne (voir figure 4.1) et à deux antennes (voir figure 4.2). Ainsi nous pourrions comparer leurs performances. Il serait aussi intéressant de tester si l'antenne d'émission supporte toute la puissance que peut fournir l'amplificateur. Cela permettrait peut-être d'augmenter la distance d'émission mais aussi de ne plus utiliser l'atténuateur variable qui ne nous a pas convaincu. Néanmoins, s'il est nécessaire de pouvoir contrôler la puissance émise par l'antenne il faudrait trouver un nouvel atténuateur variable de meilleure qualité.

Nous pourrions aussi refaire nos expérience sur la distance de communication et sur les protections de type blindage électromagnétique avec des étiquettes implémentant d'autres normes que la ISO/IEC 15693.

La technologie NFC est selon nous une piste intéressante pour supprimer les risques liés à l'utilisation de solutions RFID en application de sécurité. Nous aimerions travailler à l'élaboration de librairies cryptographiques accessibles à tous les concepteurs d'application sur appareils mobiles. Ainsi, il serait très simple pour eux de développer des applications utilisant des algorithmes cryptographiques réputés sûrs.

RÉFÉRENCES

[1] CUMMINGS, N. (2003). iCLASS Levels of Security. Consulté le 22 novembre 2012, Tiré de `http://www.norbain.co.uk/downloads/others/iCLASS-Levels.pdf`.

[2] CURTIN, M. (2005). *Brute force : cracking the data encryption standard*, Springer, chapitre 38.

[3] DE KONING GANS, G., HOEPMAN, J. et GARCIA, F. (2008). A practical attack on the MIFARE Classic. *Smart Card Research and Advanced Applications*, 267–282.

[4] EPCGLOBAL (2012). Protecting Species. *discoverrfid.org*. Consulté le 2 novembre 2012, Tiré de `http://www.securityinfowatch.com/press_release/10492011/why-walmart-is-adopting-rfid`.

[5] GARCIA, F. D., DE KONING GANS, G., MUIJRERS, R., VAN ROSSUM, P., VERDULT, R., SCHREUR, R. W. et JACOBS, B. (2008). Dismantling MIFARE Classic. S. Jajodia et J. López, éditeurs, *ESORICS*. Springer, vol. 5283 de *Lecture Notes in Computer Science*, 97–114.

[6] GARCIA, F. D., DE KONING GANS, G. et VERDULT, R. (2011). Exposing iClass Key Diversification. D. Brumley et M. Zalewski, éditeurs, *WOOT*. USENIX Association, 128–136.

[7] GARCIA, F. D., DE KONING GANS, G., VERDULT, R. et MERIAC, M. (2012). Dismantling iClass and iClass Elite. S. Foresti, M. Yung et F. Martinelli, éditeurs, *ESORICS*. Springer, vol. 7459 de *Lecture Notes in Computer Science*, 697–715.

[8] GARCIA, F. D., VAN ROSSUM, P., VERDULT, R. et SCHREUR, R. W. (2009). Wirelessly Pickpocketing a Mifare Classic Card. *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 3–15.

[9] GLOBAL, H. (2012). HID Proximity. Consulté le 3 décembre 2012, Tiré de `http://www.hidglobal.com/products/readers/hid-proximity`.

[10] HID GLOBAL (2006). iCLASS Serial Protocol Interface.

[11] HID GLOBAL (2012). Brochure iClass. Consulté le 22 novembre 2012, Tiré de `http://www.hidglobal.com/sites/hidglobal.com/files/iclass-products-br-en.pdf`.

[12] INSIDE CONTACTLESS (2004). Datasheet PicoPass 2KS. Rapport technique.

[13] JACKSON HIGGINS, K. (2008). New 'On/Off Switch' Protects RFID Cards From Hacks. *Dark Reading*. Consulté le 8 décembre

2012, Tiré de http://www.darkreading.com/security/news/211201220/new-on-off-switch-protects-rfid-cards-from-hacks.html.

[14] KASPER, M., KASPER, T., MORADI, A. et PAAR, C. (2009). Breaking KeeLoq in a flash : on extracting keys at lightning speed. *Progress in Cryptology–AFRICACRYPT 2009*, 403–420.

[15] KERCKHOFFS, A. (1883). La cryptographie militaire. *Journal des Sciences Militaires*, 9, 5–38.

[16] KFIR, Z. et WOOL, A. (2005). Picking Virtual Pockets using Relay Attacks on Contactless Smartcard. *SecureComm*. IEEE, 47–58.

[17] KIM, C., JUNG, E.-G., LEE, D. H., JUNG, C.-H. et HAN, D. (2011). Cryptanalysis of INCrypt32 in HID's iCLASS Systems. *IACR Cryptology ePrint Archive*, 469.

[18] KIRK, J. (2012). Pacemaker hack can deliver deadly 830-volt jolt. *Computerworld*. Consulté le 29 novembre 2012, Tiré de https://www.computerworld.com/s/article/9232477/Pacemaker_hack_can_deliver_deadly_830_volt_jolt?taxonomyId=85.

[19] KIRSCHENBAUM, I. et WOOL, A. (2006). How to build a low-cost, extended-range RFID skimmer. *Proceedings of the 15th conference on Security symposium*. USENIX Association, 43–57.

[20] LIFCHITZ, R. (2012). Hacking the NFC credit cards for fun and debit. Présentation au Hackito Ergo Sum 2012 à Paris.

[21] MERIAC, M. (2010). Heart of Darkness - exploring the uncharted backwaters of HID iCLASS^{TM} security. Rapport technique. Présentation au 27^{e} Chaos Computer Congress.

[22] MERIAC, M. et PLÖTZ, H. (2010). Analyzing a modern cryptographic RFID system HID iClass demystified. Présentation au 27^{e} Chaos Computer Congress.

[23] MICROCHIP (2010). PIC18FXX2/XX8 Flash Microcontroller Programming Specification.

[24] NOHL, K., EVANS, D., STARBUG, S. et PLÖTZ, H. (2008). Reverse-engineering a cryptographic RFID tag. *Proceedings of the 17th conference on Security symposium*. USENIX Association, 185–193.

[25] NOHL, K. et PLÖTZ, H. (2007). Mifare, little security, despite obscurity. Presentation on the 24th congress of the Chaos Computer Club in Berlin.

[26] RFIDEAS (2012). pcProx Writer Data Sheet. Consulté le 28 novembre 2012, Tiré de http://www.rfideas.com/downloads/pcProxWriter.pdf.

[27] SOLICORE (2010). Thin and Flexible Lithium Polymer Batteries. Consulté le 10 décembre 2012, Tiré de http://www.solicore.com/.

[28] SWEDBERG, C. (2012). McCarran International Airport Expands Its RFID Baggage-Handling System. *RFID Journal*. Consulté le 20 novembre 2012, Tiré de `http://www.rfidjournal.com/article/view/9809`.

[29] WESTHUES, J. (2010). Liste des composants de la Proxmark3. Consulté le 10 novembre 2012, Tiré de `https://proxmark3.googlecode.com/svn/trunk/doc/proxmark3.xlsf`.

[30] WESTHUES, J. (2010). Topologie de la Proxmark3. Consulté le 10 novembre 2012, Tiré de `https://proxmark3.googlecode.com/svn/trunk/doc/proxmark3.pdf`.

[31] WHITE, E. (2010). Why Walmart is adopting RFID. *Security InfoWatch*. Consulté le 2 novembre 2012, Tiré de `http://www.securityinfowatch.com/press_release/10492011/why-walmart-is-adopting-rfid`.